(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平９－１６２８５９

(43)公開日　平成９年（１９９７）６月２０日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
H04L 9/20			H04L 9/00	653	
9/16				643	
H04N 7/24			H04N 7/13	Z	
7/167			7/167	Z	

審査請求　未請求　請求項の数２３　ＯＬ　（全２７頁）

(21)出願番号　特願平７－３１９４２１

(22)出願日　平成７年（１９９５）１２月７日

(71)出願人　０００００５２２３
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　小川　清隆
神奈川県川崎市中原区上小田中１０１５番地　富士通株式会社内

(72)発明者　小桧山　清之
神奈川県川崎市中原区上小田中１０１５番地　富士通株式会社内

(74)代理人　弁理士　平戸　哲夫

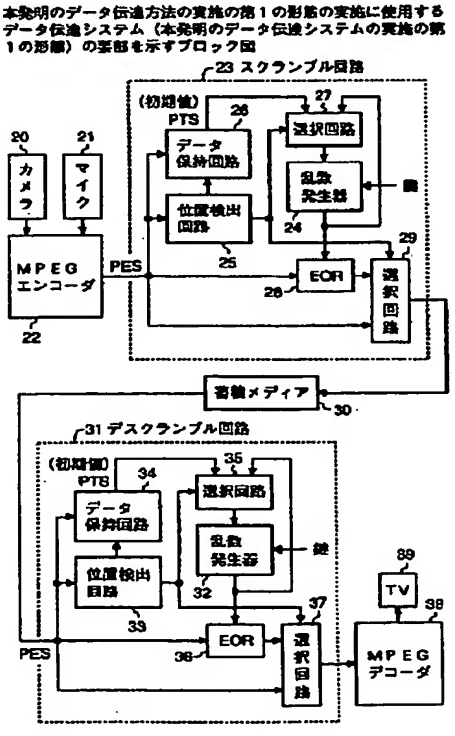
最終頁に続く

(54)【発明の名称】スクランブル方法及び装置、デスクランブル方法及び装置、並びに、データ伝達方法及びシステム

(57)【要約】

【課題】ＭＰＥＧ標準のストリームの伝達系などに適用して好適なデータ伝達システムに関し、機密性の高いデータ伝達を実現する。

【解決手段】スクランブル回路２３の乱数発生器２４には、スクランブルの対象とされているパケット・データ部のストリームごとに、値を一定としないＰＴＳ（再生出力の時刻管理情報）を初期値として供給し、デスクランブル回路３１の乱数発生器３２には、スクランブルされているパケット・データ部のストリームごとに、ＰＴＳを初期値として供給する。



1

【特許請求の範囲】

【請求項１】第１のストリーム部の後方に第２のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームのうち、スクランブルの対象とされている第２のストリーム部を乱数発生器を使用してスクランブルするスクランブル方法であって、前記スクランブルの対象とされている第２のストリーム部ごとに、前記第１のストリーム部内のデータ値が一定でない所定のデータのデータ値を初期値として前記乱数発生器に供給することにより、前記スクランブルの対象とされている第２のストリーム部をスクランブルすることを特徴とするスクランブル方法。

【請求項２】前記スクランブルの対象とされている第２のストリーム部と同一の単位ストリームの第１のストリーム部内に前記所定のデータが存在しない場合には、前記所定のデータが存在する第１のストリーム部のうち、前記所定のデータが存在しない第１のストリーム部の直前の第１のストリーム部内の前記所定のデータのデータ値を初期値として前記乱数発生器に供給することにより、前記スクランブルの対象とされている第２のストリーム部をスクランブルすることを特徴とする請求項１記載のスクランブル方法。

【請求項３】前記第１のストリーム部の後方に第２のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームは、ＭＰＥＧ標準のストリームであり、前記第１のストリーム部は、パケット・ヘッダ部のストリーム、前記第２のストリーム部は、パケット・データ部又はペイロード部のストリーム、前記所定のデータは、プレゼンテーション・タイム・スタンプ又はデコーディング・タイム・スタンプ又は巡回カウンタ又はデコーディング・タイム・スタンプと巡回カウンタとを組み合わせ又は演算したデータであることを特徴とする請求項１又は２記載のスクランブル方法。

【請求項４】前記第１のストリーム部の後方に第２のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームの全部又は一部を複数列のストリームにパラレル変換してスクランブルすることを特徴とする請求項１、２又は３記載のスクランブル方法。

【請求項５】第１のストリーム部の後方に第２のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームのうち、スクランブルの対象とされている第２のストリーム部をスクランブルするスクランブル装置であって、乱数を発生する乱数発生器と、前記スクランブルの対象とされている第２のストリーム部ごとに、前記第１のストリーム部内のデータ値が一定でない所定のデータのデータ値を初期値として前記乱数発生器に供給する初期値供給回路と、前記スクランブルの対象とされている第２のストリーム部と前記乱数発生器から出力される乱数とを論理演算して前記スクランブルの対象とされている第２のストリーム部をスクランブルする論理演算回路とを備えていることを特徴とするスクランブル装置。

2

【請求項６】前記初期値供給回路は、前記スクランブルの対象とされている第２のストリーム部と同一の単位ストリームの第１のストリーム部内に前記所定のデータが存在しない場合には、前記所定のデータが存在する第１のストリーム部のうち、前記所定のデータが存在しない第１のストリーム部の直前の第１のストリーム部内の前記所定のデータのデータ値を初期値として前記乱数発生器に供給することを特徴とする請求項５記載のスクランブル装置。

【請求項７】前記第１のストリーム部の後方に第２のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームは、ＭＰＥＧ標準のストリームであり、前記第１のストリーム部は、パケット・ヘッダ部のストリーム、前記第２のストリームは、パケット・データ部又はペイロード部のストリーム、前記所定のデータは、プレゼンテーション・タイム・スタンプ又はデコーディング・タイム・スタンプ又は巡回カウンタ又はデコーディング・タイム・スタンプと巡回カウンタとを組み合わせ又は演算したデータであることを特徴とする請求項５又は６記載のスクランブル装置。

【請求項８】前記初期値供給回路は、前記所定のデータの位置及び前記第２のストリーム部の開始位置を検出する位置検出回路と、この位置検出回路が前記所定のデータの位置を検出した場合、前記所定のデータのデータ値を保持するデータ保持回路とを備えていることを特徴とする請求項５、６又は７記載のスクランブル装置。

【請求項９】前記第１のストリーム部の後方に第２のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームを複数列のストリームにパラレル変換するシリアル／パラレル変換回路を有し、前記データ保持回路及び前記論理演算回路は、複数列のストリームに対応することができるように構成されていると共に、前記論理演算回路から出力される複数列のストリームをシリアル変換するパラレル／シリアル変換回路を備えていることを特徴とする請求項５、６、７又は８記載のスクランブル装置。

【請求項１０】前記位置検出回路による処理をＣＰＵによるソフトウエア処理により行い、規格の異なる複数のストリームに対応することができるように構成されていることを特徴とする請求項８又は９記載のスクランブル装置。

【請求項１１】第１のストリーム部の後方に第２のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームのうち、デスクランブルの対象とされている第２のストリーム部を乱数発生器を使用してデスクランブルするデスクランブル方法であって、前記デスクランブルの対象とされている第２のストリーム部ごとに、前記第１のストリーム部内のデータ値が一定で

ない所定のデータのデータ値を初期値として前記乱数発生器に供給することにより、前記デスクランブルの対象とされている第２のストリーム部をデスクランブルすることを特徴とするデスクランブル方法。

【請求項１２】前記デスクランブルの対象とされている第２のストリーム部と同一の単位ストリームの第１のストリーム部内に前記所定のデータが存在しない場合には、前記所定のデータが存在する第１のストリーム部のうち、前記所定のデータが存在しない第１のストリーム部の直前の第１のストリーム部内の前記所定のデータのデータ値を初期値として前記乱数発生器に供給することにより、前記デスクランブルの対象とされている第２のストリーム部をデスクランブルすることを特徴とする請求項１１記載のデスクランブル方法。

【請求項１３】前記第１のストリーム部の後方に第２のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームは、ＭＰＥＧ標準のストリームであり、前記第１のストリーム部は、パケット・ヘッダ部のストリーム、前記第２のストリームは、パケット・データ部又はペイロード部のストリーム、前記所定のデータは、プレゼンテーション・タイム・スタンプ又はデコーディング・タイム・スタンプ又は巡回カウンタ又はデコーディング・タイム・スタンプと巡回カウンタとを組み合わせ又は演算したデータであることを特徴とする請求項１１又は１２記載のデスクランブル方法。

【請求項１４】前記第１のストリーム部の後方に第２のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームの全部又は一部を複数のストリームにパラレル変換してデスクランブルすることを特徴とする請求項１１、１２又は１３記載のデスクランブル方法。

【請求項１５】第１のストリーム部の後方に第２のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームのうち、デスクランブルの対象とされている第２のストリーム部をデスクランブルするデスクランブル装置であって、乱数を発生する乱数発生器と、前記デスクランブルの対象とされている第２のストリーム部ごとに、前記第１のストリーム部内のデータ値が一定でない所定のデータのデータ値を初期値として前記乱数発生器に供給する初期値供給回路と、前記デスクランブルの対象とされている第２のストリーム部と前記乱数発生器から出力される乱数とを論理演算して前記デスクランブルの対象とされている第２のストリーム部をデスクランブルする論理演算回路とを備えていることを特徴とするデスクランブル装置。

【請求項１６】前記初期値供給回路は、前記デスクランブルの対象とされている第２のストリーム部と同一の単位ストリームの第１のストリーム部内に前記所定のデータが存在しない場合には、前記所定のデータが存在する第１のストリーム部のうち、前記所定のデータが存在しない第１のストリーム部の直前の第１のストリーム部内の前記所定のデータのデータ値を初期値として前記乱数発生器に供給することを特徴とする請求項１５記載のデスクランブル装置。

【請求項１７】前記第１のストリーム部の後方に第２のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームは、ＭＰＥＧ標準のストリームであり、前記第１のストリーム部は、パケット・ヘッダ部のストリーム、前記第２のストリームは、パケット・データ部又はペイロード部のストリーム、前記所定のデータは、プレゼンテーション・タイム・スタンプ又はデコーディング・タイム・スタンプ又は巡回カウンタ又はデコーディング・タイム・スタンプと巡回カウンタとを組み合わせ又は演算したデータであることを特徴とする請求項１５又は１６記載のデスクランブル装置。

【請求項１８】前記初期値供給回路は、前記所定のデータの位置及び前記第２のストリーム部の開始位置を検出する位置検出回路と、この位置検出回路が前記所定のデータの位置を検出した場合、前記所定のデータのデータ値を保持するデータ保持回路とを備えていることを特徴とする請求項１５、１６又は１７記載のデスクランブル装置。

【請求項１９】前記第１のストリーム部の後方に第２のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームを複数列のストリームにパラレル変換するシリアル／パラレル変換回路を有し、前記データ保持回路及び前記論理演算回路は、複数列のストリームに対応することができるように構成されていると共に、前記論理演算回路から出力される複数列のストリームをシリアル変換するパラレル／シリアル変換回路を備えていることを特徴とする請求項１５、１６，１７又は１８記載のデスクランブル装置。

【請求項２０】前記位置検出回路による処理をＣＰＵによるソフトウエア処理により行い、規格の異なる複数のストリームに対応することができるように構成されていることを特徴とする請求項１８又は１９記載のデスクランブル装置。

【請求項２１】カード化されると共に、身分証明データを記憶する記憶回路を有し、外部装置から前記身分証明データを認証した場合のみ、前記外部装置から前記乱数発生器にアクセスできるように構成されていることを特徴とする請求項１５、１６又は１７記載のデスクランブル装置。

【請求項２２】伝達元において、第１のストリーム部の後方に第２のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームについて、請求項１、２、３又は４記載のスクランブル方法を実行し、これにより得られるストリームを伝達メディアを介して伝達先に伝達し、前記伝達先において請求項１１、１２、１３又は１４記載のデスクランブル方法を実行し、

5

前記第１のストリーム部の後方に第２のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームを復元する工程を含んでいることを特徴とするデータ伝達方法。

【請求項２３】請求項５、６、７、８、９又は１０記載のスクランブル装置を有し、第１のストリーム部の後方に第２のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームをスクランブルの対象とされている第２のストリーム部をスクランブルしてなるストリームに変換して伝達メディアに伝達する伝達元と、請求項１５、１６、１７、１８、１９、２０又は２１記載のデスクランブル装置を有し、前記伝達メディアから供給されるストリームを前記第１のストリーム部の後方に第２のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームに復元する伝達先とを備えていることを特徴とするデータ伝達システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ディジタル動画像符号化（圧縮）、音響符号化及びその多重・分離方法についての国際標準であるＭＰＥＧ（Moving Picture Experts Group）標準のストリーム（ビット列）の伝達系などに適用して好適なスクランブル方法及び装置、デスクランブル方法及び装置、並びに、データ伝達方法及びシステムに関する。

【０００２】

【従来の技術】従来、データ伝達システムとして、例えば、図１２に、その要部を示すようなものが知られている。

【０００３】図１２中、１は映像データを得るためのカメラ、２は音声データを得るためのマイク、３はカメラ１により得られる映像データとマイク２により得られる音声データとを符号化して時分割多重し、付加データを配列したパケット・ヘッダ部と、映像データや音声データを配列したパケット・データ部とからなるＭＰＥＧ標準のストリームにエンコードするＭＰＥＧエンコーダである。

【０００４】また、４はＭＰＥＧエンコーダ３から出力されるストリームをパケット・データ部のストリームがスクランブルされてなるストリームに変換するスクランブル回路である。

【０００５】このスクランブル回路４において、５は鍵信号により指定される系列の乱数を発生する乱数発生器、６はＭＰＥＧエンコーダ３から出力されるストリームのうちのパケット・データ部のストリームと乱数発生器５から出力される乱数とを排他的論理和（以下、ＥＯＲという）処理するＥＯＲ回路である。

【０００６】また、７はＭＰＥＧエンコーダ３から出力されるストリームのうちのパケット・ヘッダ部のストリ

6

ームと、ＥＯＲ回路６から出力されるストリームとを選択して出力する選択回路である。

【０００７】また、８はディスク、テープ等の蓄積メディアや、衛星放送、ＣＡＴＶ等の放送メディア等、スクランブル回路４から出力されるストリームの伝達媒体である伝達メディアである。

【０００８】また、９は伝達メディア８を介して伝達されるスクランブル回路４から出力されたストリームをパケット・データ部のストリームがデスクランブルされてなるストリームに変換するデスクランブル回路である。

【０００９】このデスクランブル回路９において、１０は乱数発生器５と同一の回路構成の乱数発生器であり、この乱数発生器１０には乱数発生器５に使用された鍵信号と同一内容の鍵信号が供給される。

【００１０】また、１１は伝達メディア８を介して伝達されるスクランブル回路４から出力されたストリームのうちのパケット・データ部のストリームと、乱数発生器１０から出力される乱数とをＥＯＲ処理するＥＯＲ回路である。

【００１１】また、１２は伝達メディア８を介して伝達されるスクランブル回路４から出力されたストリームのうちのパケット・ヘッダ部のストリームと、ＥＯＲ回路１１から出力されるストリームとを選択して出力する選択回路である。

【００１２】また、１３はデスクランブル回路９から出力されるストリームから映像データと音声データとを分離し、更に、これらを復号化するＭＰＥＧデコーダ、１４はＭＰＥＧデコーダ１３から出力される映像データ及び音声データが供給されるテレビジョン受像機（ＴＶ）である。

【００１３】このデータ伝達システムは、ＭＰＥＧエンコーダ３から出力されるＭＰＥＧ標準のストリームをパケット・データ部のストリームをスクランブルしてなるストリームとして伝達することによって、不法なコピーからパケット・データを保護しようとするものである。

【００１４】

【発明が解決しようとする課題】しかし、このデータ伝達システムにおいては、例えば、図１３に示すように、ＭＰＥＧエンコーダ３からパケット・データ部のストリームとしてａ１、ａ２、ａ３・・・が出力されると共に、乱数発生器５、１０から乱数ｃ１、ｃ２、ｃ３・・・が出力される場合、ＥＯＲ回路６の出力は、

【００１５】

【数１】

$$a1 \oplus c1,\ a2 \oplus c2,\ a3 \oplus c3 \cdots$$

【００１６】となり、これが選択回路７から出力され、ＥＯＲ回路１１に入力されることになるので、ＥＯＲ回路１１から出力されるストリームは、ａ１、ａ２、ａ３・・・となる。したがって、ＥＯＲ回路１１に入力されるストリーム

7

【００１７】

【数２】

$$a1 \oplus c1,\ a2 \oplus c2,\ a3 \oplus c3 \cdots$$

【００１８】と、ＥＯＲ回路１１から出力されるストリームａ１、ａ２、ａ３・・・とをＥＯＲ回路１５でＥＯＲ処理すると、乱数発生器１０から出力される乱数ｃ１、ｃ２、ｃ３・・・を得ることができる。

【００１９】このように、このデータ伝達システムにおいては、鍵信号が不明でも、乱数発生器１０から出力される乱数パターンが容易にコピーされてしまい、スクランブルされたパケット・データについてもデスクランブルされてしまうおそれがあるという問題点があった。

【００２０】本発明は、かかる点に鑑み、機密性の高いデータ伝達を実現することができるようにしたスクランブル方法及び装置、デスクランブル方法及び装置、並びに、データ伝達方法及びシステムを提供することを目的とする。

【００２１】

【課題を解決するための手段】本発明のスクランブル方法は、第１のストリーム部の後方に第２のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームのうち、スクランブルの対象とされている第２のストリーム部を乱数発生器を使用してスクランブルするスクランブル方法であって、前記スクランブルの対象とされている第２のストリーム部ごとに、前記第１のストリーム部内のデータ値が一定でない所定のデータのデータ値を初期値として前記乱数発生器に供給することにより、前記スクランブルの対象とされている第２のストリーム部をスクランブルするするというものである。

【００２２】本発明のスクランブル方法を使用する場合には、デスクランブルは、スクランブルされている第２のストリーム部ごとに、第１のストリーム部内のデータ値が一定でない所定のデータのデータ値を初期値として乱数発生器に供給することにより行われることになる。

【００２３】即ち、デスクランブル側の乱数発生器には、スクランブルされている第２のストリーム部ごとに、値を一定としない初期値が供給されることになるので、乱数発生器から発生される乱数パターンを解析することが困難となり、機密性の高いデータ伝達を実現することができる。

【００２４】また、本発明のスクランブル装置は、第１のストリーム部の後方に第２のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームのうち、スクランブルの対象とされている第２のストリーム部をスクランブルするスクランブル装置であって、乱数を発生する乱数発生器と、前記スクランブルの対象とされている第２のストリーム部ごとに、前記第１のストリーム部内のデータ値が一定でない所定のデータのデータ値を初期値として前記乱数発生器に供給する初期値供給回路と、前記スクランブルの対象とされている第２のストリーム部と前記乱数発生器から出力される乱数とを論理演算して前記スクランブルの対象とされている第２のストリーム部をスクランブルする論理演算回路とを備えて備えというものである。

【００２５】本発明のスクランブル装置を使用する場合には、デスクランブル装置は、乱数を発生する乱数発生器と、スクランブルされている第２のストリーム部ごとに、第１のストリーム部内のデータ値が一定でない所定のデータのデータ値を初期値として乱数発生器に供給する初期値供給回路と、スクランブルされている第２のストリーム部と乱数発生器から出力される乱数とを論理演算してスクランブルされている第２のストリーム部をデスクランブルする論理演算回路とを備えて構成されることになる。

【００２６】即ち、デスクランブル装置の乱数発生器には、スクランブルされている第２のストリーム部ごとに、値を一定としない初期値が供給されることになるので、乱数発生器から発生される乱数パターンを解析することが困難となり、機密性の高いデータ伝達を実現することができる。

【００２７】また、本発明のデスクランブル方法は、第１のストリーム部の後方に第２のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームのうち、デスクランブルの対象とされている第２のストリーム部を乱数発生器を使用してデスクランブルするデスクランブル方法であって、前記デスクランブルの対象とされている第２のストリーム部ごとに、前記第１のストリーム部内のデータ値が一定でない所定のデータのデータ値を初期値として前記乱数発生器に供給することにより、前記デスクランブルの対象とされている第２のストリーム部をデスクランブルするというものである。

【００２８】本発明のデスクランブル方法によれば、乱数発生器には、スクランブルされている第２のストリーム部ごとに、値を一定としない初期値が供給されることになるので、乱数発生器から発生される乱数パターンを解析することが困難となり、機密性の高いデータ伝達を実現することができる。

【００２９】また、本発明のデスクランブル装置は、第１のストリーム部の後方に第２のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームのうち、デスクランブルの対象とされている第２のストリーム部をデスクランブルするデスクランブル装置であって、乱数を発生する乱数発生器と、前記デスクランブルの対象とされている第２のストリーム部ごとに、前記第１のストリーム部内のデータ値が一定でない所定のデータのデータ値を初期値として前記乱数発生器に供給する初期値供給回路と、前記デスクランブルの対象とされている第２のストリーム部と前記乱数発生器から出

力される乱数とを論理演算して前記デスクランブルの対象とされている第２のストリーム部をデスクランブルする論理演算回路とを備えるというものである。

【００３０】本発明のデスクランブル装置によれば、乱数発生器には、スクランブルされている第２のストリーム部ごとに、値を一定としない初期値が供給されることになるので、乱数発生器から発生される乱数パターンを解析することが困難となり、機密性の高いデータ伝達を実現することができる。

【００３１】また、本発明のデータ伝達方法は、伝達元において、第１のストリーム部の後方に第２のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームについて、本発明のスクランブル方法を実行し、これにより得られるストリームを伝達メディアを介して伝達先に伝達し、伝達先において本発明ののデスクランブル方法を実行し、第１のストリーム部の後方に第２のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームを復元する工程を含むというものである。

【００３２】本発明のデータ伝達方法によれば、本発明のスクランブル方法及び本発明のデスクランブル方法を使用しているので、機密性の高いデータ伝達を実現することができる。

【００３３】本発明のデータ伝達システムは、本発明のスクランブル装置を有し、第１のストリーム部の後方に第２のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームをスクランブルの対象とされている第２のストリーム部をスクランブルしてなるストリームに変換して伝達メディアに伝達する伝達元と、本発明のデスクランブル装置を有し、伝達メディアから供給されるストリームを第１のストリーム部の後方に第２のストリーム部を配列したストリームを単位ストリームとして連ねてなるストリームに復元する伝達先とを備えて構成されるものである。

【００３４】本発明のデータ伝達装置によれば、本発明のスクランブル装置及び本発明のデスクランブル装置を使用しているので、機密性の高いデータ伝達を実現することができる。

【００３５】

【発明の実施の形態】以下、図１～図１１を参照して、本発明のデータ伝達方法及びシステムの実施の第１の形態～第５の形態について、本発明のスクランブル方法及び装置並びに本発明のデスクランブル方法及び装置の実施の形態を含めて説明する。

【００３６】第１の形態・・図１～図４

図１は本発明のデータ伝達方法の実施の第１の形態の実施に使用するデータ伝達システム（本発明のデータ伝達システムの実施の第１の形態）の要部を示すブロック図である。

【００３７】図１中、２０は映像データを得るためのカメラ、２１は音声データを得るためのマイク、２２はカメラ２０により得られる映像データとマイク２１により得られる音声データとを符号化して時分割多重し、ＭＰＥＧ２－ＰＳ（プログラム・ストリーム）標準に基づくストリームにエンコードするＭＰＥＧエンコーダである。

【００３８】図２は、ＭＰＥＧ２－ＰＳのＰＥＳ（Packetized Elementary Stream）パケットの構造を示す図である。図２中、ＰＴＳ（Presentation Time Stamp）は再生出力の時刻管理情報であり、一般に、７００ｍｓごとに挿入される。

【００３９】また、ＤＴＳ（Decoding Time Stamp）は復号の時刻管理情報、ＰＥＳスクランブル制御はスクランブル制御の有無を表示するデータ、ＰＴＳ＆ＤＴＳフラグはＰＴＳデータが存在するか否かを示すフラグである。

【００４０】また、図１において、２３はＭＰＥＧエンコーダ２２から出力されるストリームをスクランブルの対象とされているパケット・データ部のストリームがスクランブルされてなるストリームに変換するスクランブル回路である。

【００４１】このスクランブル回路２３は、本発明のスクランブル方法の実施の第１の形態の実施に使用するスクランブル装置であり、本発明のスクランブル装置の実施の第１の形態をなすものである。

【００４２】スクランブル回路２３において、２４は鍵信号により指定される系列の乱数を発生するＤＥＳ（Data Encryption Standard）規格の乱数発生器、２５はＭＰＥＧエンコーダ２２から出力されるストリームを入力し、パケット開始コードの検出、ＰＥＳスクランブル制御の内容の確認、ＰＴＳ＆ＤＴＳフラグの確認、ＰＴＳの位置検出及びパケット・データ部の開始位置検出などを行う位置検出回路である。

【００４３】また、２６はＰＴＳデータを保持するデータ保持回路であり、このデータ保持回路２６は、位置検出回路２５がＰＴＳの位置を検出すると、この位置検出したＰＴＳのデータを保持するように位置検出回路２５により制御される。

【００４４】また、２７はデータ保持回路２６が保持するＰＴＳデータ又は乱数発生器２４から出力される乱数自身を乱数発生器２４に供給する選択回路であり、この選択回路２７は、位置検出回路２５がスクランブルの対象とされているパケット・データ部の開始位置を検出すると、データ保持回路２６が保持するＰＴＳデータを初期値として乱数発生器２４に供給し、その後、パケット・データ部のストリームが終了するまで、乱数発生器２４から出力される乱数をフィードバックするように位置検出回路２５により制御される。

【００４５】なお、これら位置検出回路２５と、データ保持回路２６と、選択回路２７とでスクランブル回路２

３における初期値供給回路が構成されている。

【００４６】また、２８はＭＰＥＧエンコーダ２２から出力されるストリームのうち、スクランブルの対象とされているパケット・データ部のストリームと乱数発生器２４から出力される乱数とをＥＯＲ処理し、スクランブルの対象とされているパケット・データ部のストリームをスクランブルするＥＯＲ回路である。

【００４７】また、２９はＭＰＥＧエンコーダ２２から出力されるストリームとＥＯＲ回路２８から出力されるストリームとを選択して出力する選択回路であり、この選択回路２９は、ＭＰＥＧエンコーダ２２から出力されるストリームをスクランブルの対象とされているパケット・データ部のストリームがスクランブルされてなるストリームに変換したストリームを出力するように位置検出回路２５により制御される。

【００４８】また、３０は選択回路２９から出力されるストリーム、即ち、スクランブル回路２３から出力されるストリームを蓄積するディスク等の蓄積メディア、３１は蓄積メディア３０から供給されるストリームをスクランブルされているパケット・データ部のストリームがデスクランブルされてなるストリームに変換するデスクランブル回路である。

【００４９】このデスクランブル回路３１は、本発明のデスクランブル方法の実施の第１の形態の実施に使用するデスクランブル装置であり、本発明のデスクランブル装置の実施の第１の形態をなすものである。

【００５０】このデスクランブル回路３１において、３２は乱数発生器２４と同一の回路構成の乱数発生器であり、この乱数発生器３２には乱数発生器２４に使用された鍵信号と同一内容の鍵信号が供給される。

【００５１】また、３３は蓄積メディア３０から供給されるストリームを入力し、パケット開始コードの検出、ＰＥＳスクランブル制御の内容の確認、ＰＴＳ＆ＤＴＳフラグの確認、ＰＴＳの位置検出及びパケット・データ部の開始位置検出などを行う位置検出回路である。

【００５２】また、３４はＰＴＳデータを保持するデータ保持回路であり、このデータ保持回路３４は、位置検出回路３３がＰＴＳの位置を検出すると、この位置検出したＰＴＳのデータを保持するように位置検出回路３３により制御される。

【００５３】また、３５はデータ保持回路３４が保持するＰＴＳデータ又は乱数発生器３２から出力される乱数自身を乱数発生器３２に供給する選択回路であり、この選択回路３５は、位置検出回路３３がデスクランブルの対象、即ち、スクランブルされているパケット・データ部の開始位置を検出すると、データ保持回路３４が保持するＰＴＳデータを初期値として乱数発生器３２に供給し、その後、パケット・データ部のストリームが終了するまで、乱数発生器３２から出力される乱数をフィードバックするように位置検出回路３３により制御される。

【００５４】なお、これら位置検出回路３３と、データ保持回路３４と、選択回路３５とでデスクランブル回路３１における初期値供給回路が構成されている。

【００５５】また、３６は蓄積メディア３０から供給されるストリームのうち、スクランブルされているパケット・データ部のストリームと乱数発生器３２から出力される乱数とをＥＯＲ処理し、スクランブルされているパケット・データ部のストリームをデスクランブルするＥＯＲ回路である。

【００５６】また、３７は蓄積メディア３０から供給されるストリームと、ＥＯＲ回路３６から出力されるストリームとを選択して出力する選択回路であり、この選択回路３７は、蓄積メディア３０から供給されるストリームをスクランブルされているパケット・データ部のストリームがデスクランブルされてなるストリームに変換したストリームを出力するように位置検出回路３３により制御される。

【００５７】また、３８は選択回路３７から出力されるストリーム、即ち、デスクランブル回路３１から出力されるストリームから映像データのストリームと音声データのストリームとを分離して復号化するＭＰＥＧデコーダ、３９はＭＰＥＧデコーダ３８から出力される映像データ及び音声データが供給されるテレビジョン受像機である。

【００５８】このデータ伝達システムにおいては、カメラ２０により得られる映像データとマイク２１により得られる音声データとは、ＭＰＥＧエンコーダ２２によって、ＭＰＥＧ２－ＰＳ標準に基づくストリームにエンコードされ、スクランブル回路２３に入力され、位置検出回路２５、データ保持回路２６、ＥＯＲ回路２８及び選択回路２９に供給される。

【００５９】図３はスクランブル回路２３の動作（本発明のスクランブル方法の実施の第１の形態）を説明するためのフローチャートであり、スクランブル回路２３においては、同一動作が繰り返して行われるので、選択回路２９からスクランブルの対象とされているパケット・データ部のストリームの出力を終了した時から動作を説明すると、位置検出回路２５は、ＭＰＥＧエンコーダ２２から入力されるストリームをそのまま出力し続けるように選択回路２９を制御し（ステップＳ１）、パケット開始コードを検出するための状態となる（ステップＳ２）。

【００６０】そして、位置検出回路２５は、パケット開始コードを検出した場合、パケット・ヘッダ部のスクランブル制御の内容からパケット・データ部のストリームがスクランブルの対象であるか否かを判断し（ステップＳ３）、スクランブルの対象とされていない場合（ＮＯの場合）には、動作はステップＳ２に戻り、位置検出回路２５は、パケット開始コードを検出するための状態となる。

【００６１】これに対して、パケット・データ部のストリームがスクランブルの対象とされている場合（ステップＳ３において、ＹＥＳの場合）には、位置検出回路２５は、パケット・ヘッダ部のＰＴＳ＆ＤＴＳフラグが“１０”又は“１１”であるか否か、即ち、ＰＴＳデータの有無を判断する（ステップＳ４）。

【００６２】判断の結果、ＰＴＳ＆ＤＴＳフラグが“１０”又は“１１”の場合、即ち、ＰＴＳデータが存在する場合には、位置検出回路２５は、ＰＴＳの位置を検出して、ＰＴＳデータをデータ保持回路２６に保持させ（ステップＳ５）、パケット・データ部の開始位置を検出するための状態となる（ステップＳ６）。

【００６３】これに対して、ＰＴＳ＆ＤＴＳフラグが“１０”又は“１１”以外の場合、即ち、ＰＴＳデータが存在しない場合には、位置検出回路２５は、そのまま、パケット・データ部の開始位置を検出するための状態となる（ステップＳ６）。

【００６４】そして、位置検出回路２５は、パケット・データ部の開始位置を検出すると、データ保持回路２６が保持するＰＴＳデータ、即ち、スクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部のＰＴＳのデータ、あるいは、スクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部にＰＴＳが存在しない場合には、ＰＴＳが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のＰＴＳデータを初期値として乱数発生器２４に供給するように選択回路２７を制御する（ステップＳ７）。

【００６５】ここに、ＥＯＲ回路２８においては、ＭＰＥＧエンコーダ２２から出力されるストリームのうち、スクランブルの対象とされているパケット・データ部のストリームと、乱数発生器２４から出力される乱数とがＥＯＲ処理され、スクランブルの対象とされているパケット・データ部のストリームのスクランブルが行われる。

【００６６】そこで、位置検出回路２５は、選択回路２９を制御して、ＥＯＲ回路２８から出力されるスクランブルされたストリームを出力し続けさせ（ステップＳ８）、パケット・データ部のストリームが終了するまで待ち（ステップＳ９）、ステップＳ１に戻る。

【００６７】このようにして、ＭＰＥＧエンコーダ２２から出力されるストリームは、スクランブルの対象とされているパケット・データ部のストリームがスクランブルされてなるストリームに変換されて蓄積メディア３０に蓄積され、この蓄積メディア３０に蓄積されたストリームは、適宜、デスクランブル回路３１に供給されることになる。

【００６８】図４はデスクランブル回路３１の動作（本発明のデスクランブル方法の実施の第１の形態）を説明するためのフローチャートであり、デスクランブル回路

３１においては、同一動作が繰り返して行われるので、選択回路３７からデスクランブルの対象とされているパケット・データ部のストリームの出力を終了した時から動作を説明すると、位置検出回路３３は、蓄積メディア３０から供給されるストリームをそのまま出力し続けるように選択回路３７を制御し（ステップＰ１）、パケット開始コードを検出するための状態となる（ステップＰ２）。

【００６９】そして、位置検出回路３３は、パケット開始コードを検出した場合、パケット・ヘッダ部のスクランブル制御の内容からパケット・データ部のストリームがデスクランブルの対象とされているか否か、即ち、スクランブルされているか否かを判断し（ステップＰ３）、スクランブルされていない場合（ＮＯの場合）には、動作はステップＰ２に戻り、位置検出回路３３は、パケット開始コードを検出するための状態となる。

【００７０】これに対して、パケット・データ部のストリームがスクランブルされている場合（ステップＰ３において、ＹＥＳの場合）には、位置検出回路３３は、パケット・ヘッダ部のＰＴＳ＆ＤＴＳフラグが“１０”又は“１１”であるか否か、即ち、ＰＴＳデータの有無を判断する（ステップＰ４）。

【００７１】判断の結果、ＰＴＳ＆ＤＴＳフラグが“１０”又は“１１”の場合、即ち、ＰＴＳデータが存在する場合には、位置検出回路３３は、ＰＴＳの位置を検出して、ＰＴＳデータをデータ保持回路３４に保持させ（ステップＰ５）、パケット・データ部の開始位置を検出するための状態となる（ステップＰ６）。

【００７２】これに対して、ＰＴＳ＆ＤＴＳフラグが“１０”又は“１１”以外の場合、即ち、ＰＴＳデータが存在しない場合には、位置検出回路３３は、そのまま、パケット・データ部の開始位置を検出するための状態となる（ステップＰ６）。

【００７３】そして、位置検出回路３３は、パケット・データ部の開始位置を検出すると、データ保持回路３４が保持するＰＴＳデータ、即ち、デスクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部のＰＴＳのデータ、あるいは、デスクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部にＰＴＳが存在しない場合には、ＰＴＳが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のＰＴＳデータを初期値として乱数発生器３２に供給するように選択回路３５を制御する（ステップＰ７）。

【００７４】ここに、ＥＯＲ回路３６では、蓄積メディア３０から供給されるストリームのうち、スクランブルされているパケット・データ部のストリームと、乱数発生器３２から出力される乱数とがＥＯＲ処理され、スクランブルされているパケット・データ部のストリームのデスクランブルが行われる。

【００７５】そこで、位置検出回路３３は、選択回路３７を制御し、ＥＯＲ回路３６から出力されるデスクランブルされたストリームを出力し続けさせ（ステップＰ８）、パケット・データ部のストリームが終了するまで待ち（ステップＰ９）、ステップＰ１に戻る。

【００７６】このようにして、蓄積メディア３０から供給されるストリームは、スクランブルされているパケット・データ部のストリームがデスクランブルされてなるストリームに変換され、ＭＰＥＧデコーダ３８に伝達される。

【００７７】ＭＰＥＧデコーダ３８においては、デスクランブル回路３１から伝達されるストリームから映像データのストリームと音声データのストリームとが分離されて復号化され、これら復号化された映像データ及び音声データは、テレビジョン受像機３９に伝達される。

【００７８】このように、本発明のデータ伝達方法及びシステムの実施の第１の形態においては、ＭＰＥＧエンコーダ２２から出力されるＭＰＥＧ２－ＰＳ標準のストリームは、スクランブル回路２３において、スクランブルの対象とされているパケット・データ部のストリームをスクランブルしてなるストリームに変換され、蓄積メディア３０を介して、デスクランブル回路３１に供給され、デスクランブルが行われて、ＭＰＥＧデコーダ３８に伝達される。

【００７９】ここに、スクランブル回路２３においては、スクランブルの対象とされているパケット・データ部のストリームごとに、スクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部のＰＴＳのデータ、あるいは、スクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部にＰＴＳが存在しない場合には、ＰＴＳが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のＰＴＳのデータ値を初期値として乱数発生器２４に供給することにより、スクランブルの対象とされているパケット・データ部のストリームのスクランブルが行われる。

【００８０】この結果、デスクランブル回路３１においては、スクランブルされているパケット・データ部のストリームごとに、デスクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部のＰＴＳのデータ、あるいは、デスクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部にＰＴＳが存在しない場合には、ＰＴＳが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のＰＴＳのデータ値を初期値として乱数発生器３２に供給することにより、スクランブルされているパケット・データ部のストリームのデスクランブルが行われることになる。

【００８１】このように、本発明のデータ伝達方法及びシステムの実施の第１の形態によれば、デスクランブル回路３１の乱数発生器３２には、スクランブルされているパケット・データ部のストリームごとに、データ値を一定としないＰＴＳのデータ値が初期値として供給されることになるので、乱数発生器３２から発生される乱数パターンを解析することが困難となり、機密性の高いデータ伝達を実現することができる。

【００８２】第２の形態・・図５～図８

図５は本発明のデータ伝達方法の実施の第２の形態の実施に使用するデータ伝達システム（本発明のデータ伝達システムの実施の第２の形態）の要部を示すブロック図である。

【００８３】図５中、４１は映像データを得るためのカメラ、４２は音声データを得るためのマイク、４３はカメラ４１により得られる映像データとマイク４２により得られる音声データとを符号化して時分割多重し、ＭＰＥＧ２－ＴＳ（トランスポート・ストリーム）標準に基づくストリームにエンコードするＭＰＥＧエンコーダである。

【００８４】図６はＭＰＥＧ２－ＴＳのトランスポート・パケットの構造を示す図であり、ＰＣＲ（Ｐrogram Ｃlock Ｒeference）はＭＰＥＧデコーダにおいて、時刻標準となるＳＴＣ（基本となる同期信号）の値をＭＰＥＧエンコーダ４３で意図した値にセット・校正するための情報である。なお、ＰＣＲは、一般に、１００ｍｓごとに挿入される。

【００８５】また、アダプテーションフラグはアダプテーション・フィールドの有無を示すフラグ、ペイロードフラグはペイロードの有無を示すフラグ、ＰＣＲフラグはＰＣＲがあるか否かを示すフラグである。

【００８６】また、図５において、４４はＭＰＥＧエンコーダ４３から出力されるストリームをスクランブルの対象とされているペイロード部のストリームがスクランブルされてなるストリームに変換するスクランブル回路である。

【００８７】このスクランブル回路４４は、本発明のスクランブル方法の実施の第２の形態の実施に使用するスクランブル装置であり、本発明のスクランブル装置の実施の第２の形態をなすものである。

【００８８】スクランブル回路４４において、４５は鍵信号により指定される系列の乱数を発生するＤＥＳ規格の乱数発生器、４６はＭＰＥＧエンコーダ４３から出力されるストリームに含まれている同期バイトの検出、アダプテーションフラグの内容の確認、ペイロードフラグの内容の確認、ＰＣＲフラグの内容の確認、ＰＣＲの位置検出及びペイロード部の開始位置検出などを行う位置検出回路である。

【００８９】また、４７はＰＣＲデータを保持するデータ保持回路であり、このデータ保持回路４７は、位置検出回路４６がＰＣＲの位置を検出すると、この位置検出したＰＣＲのデータを保持するように位置検出回路４６

により制御される。

【００９０】また、４８はデータ保持回路４７が保持するＰＣＲデータ又は乱数発生器４５から出力される乱数自身を乱数発生器４５に供給する選択回路であり、この選択回路４８は、位置検出回路４６がスクランブルの対象のペイロード部の開始位置を検出すると、データ保持回路４７が保持するＰＣＲデータを初期値として乱数発生器４５に供給し、その後、ペイロード部のストリームが終了するまで、乱数発生器４５から出力される乱数をフィードバックするように位置検出回路４６により制御される。

【００９１】なお、これら位置検出回路４６と、データ保持回路４７と、選択回路４８とでスクランブル回路４４における初期値供給回路が構成されている。

【００９２】また、４９はＭＰＥＧエンコーダ４３から出力されるストリームのうち、スクランブルの対象とされているペイロード部のストリームと乱数発生器４５から出力される乱数とをＥＯＲ処理し、スクランブルの対象とされているペイロード部のストリームをスクランブルするＥＯＲ回路である。

【００９３】また、５０はＭＰＥＧエンコーダ４３から出力されるストリームとＥＯＲ回路４９から出力されるストリームとを選択して出力する選択回路であり、この選択回路５０は、ＭＰＥＧエンコーダ４３から出力されるストリームをスクランブルの対象とされているペイロード部のストリームがスクランブルされてなるストリームに変換したストリームを出力するように位置検出回路４６により制御される。

【００９４】また、５１は選択回路５０から出力されるストリーム、即ち、スクランブル回路４４から出力されるストリームをディジタル変調するディジタル変調器、５２はディジタル変調器５１の出力を送信するためのアップ・コンバータ、５３は送信側のアンテナである。

【００９５】また、５４は受信側のアンテナ、５５は選局を行うチューナ、５６はチューナ５５によって選局した信号をディジタル復調するディジタル復調器である。

【００９６】また、５７はディジタル復調器５６から出力されるストリームをスクランブルされているペイロード部のストリームをデスクランブルしたストリームに変換するデスクランブル回路である。

【００９７】このデスクランブル回路５７は、本発明のデスクランブル方法の実施の第２の形態の実施に使用するデスクランブル装置であり、本発明のデスクランブル装置の実施の第２の形態をなすものである。

【００９８】デスクランブル回路５７において、５８は乱数発生器４５と同一の回路構成の乱数発生器であり、この乱数発生器５８には乱数発生器４５に使用された鍵信号と同一内容の鍵信号が供給される。

【００９９】また、５９はディジタル復調器５６から出力されるストリームに含まれている同期バイトの検出、

アダプテーションフラグの内容の確認、ペイロードフラグの内容の確認、ＰＣＲフラグの内容の確認、ＰＣＲの位置検出及びペイロード部の開始位置検出などを行う位置検出回路である。

【０１００】また、６０はＰＣＲデータを保持するデータ保持回路であり、このデータ保持回路６０は、位置検出回路５９がＰＣＲの位置を検出すると、この位置検出したＰＣＲのデータを保持するように位置検出回路５９により制御される。

【０１０１】また、６１はデータ保持回路６０が保持するＰＣＲデータ又は乱数発生器５８から出力される乱数自身を乱数発生器５８に供給する選択回路であり、この選択回路６１は、位置検出回路５９がデスクランブルの対象、即ち、スクランブルされているペイロード部の位置を検出すると、データ保持回路６０が保持するＰＣＲデータを初期値として乱数発生器５８に供給し、その後、ペイロード部のストリームが終了するまで、乱数発生器５８から出力される乱数をフィードバックするように位置検出回路５９により制御される。

【０１０２】なお、これら位置検出回路５９と、データ保持回路６０と、選択回路６１とでデスクランブル回路５７における初期値供給回路が構成されている。

【０１０３】また、６２はディジタル復調器５６から入力されるストリームのうち、スクランブルされているペイロード部のストリームと乱数発生器５８から出力される乱数とをＥＯＲ処理し、スクランブルされているペイロード部のストリームをデスクランブルするＥＯＲ回路である。

【０１０４】また、６３はディジタル復調器５６から出力されるストリームと、ＥＯＲ回路６２から出力されるストリームとを選択して出力する選択回路であり、この選択回路６３は、ディジタル復調器５６から出力されるストリームをスクランブルされているペイロード部のストリームがデスクランブルされてなるストリームに変換したストリームを出力するように位置検出回路５９により制御される。

【０１０５】また、６４は選択回路６３から出力されるストリーム、即ち、デスクランブル回路５７から出力されるストリームから映像データのストリームと音声データのストリームとを分離して復号化するＭＰＥＧデコーダ、６５はＭＰＥＧデコーダ６４から出力される映像データ及び音声データが供給されるテレビジョン受像機である。

【０１０６】このデータ伝達システムにおいては、カメラ４１により得られる映像データとマイク４２により得られる音声データとは、ＭＰＥＧエンコーダ４３によって、ＭＰＥＧ２－ＴＳ標準に基づくストリームにエンコードされてスクランブル回路４４に入力され、位置検出回路４６、データ保持回路４７、ＥＯＲ回路４９及び選択回路５０に供給される。

19

【０１０７】図７はスクランブル回路４４の動作（本発明のスクランブル方法の実施の第２の形態）を説明するためのフローチャートであり、スクランブル回路４４においては、同一動作が繰り返して行われるので、選択回路５０からスクランブルの対象とされているペイロード部のストリームの出力を終了した時から動作を説明すると、位置検出回路４６は、ＭＰＥＧエンコーダ４３から入力されるストリームをそのまま出力し続けるように選択回路５０を制御し、同期バイトを検出するための状態となる（ステップＮ１）。

【０１０８】そして、位置検出回路４６は、同期バイトを検出した場合、パケット・ヘッダ部のスクランブル制御の内容からペイロード部のストリームがスクランブルの対象とされているか否かを判断し（ステップＮ２）、スクランブルの対象とされていない場合（ＮＯの場合）には、動作はステップＮ１に戻り、位置検出回路４６は、同期バイトを検出するための状態となる。

【０１０９】これに対して、ペイロード部のストリームがスクランブルの対象とされている場合（ステップＮ３において、ＹＥＳの場合）には、位置検出回路４６は、アダプテーション・フラグからアダプテーション・フィールドがあるか否かを判断する（ステップＮ３）。

【０１１０】判断の結果、アダプテーション・フィールドがある場合（ＹＥＳの場合）には、位置検出回路４６は、ＰＣＲフラグからＰＣＲがあるか否かを判断し（ステップＮ４）、ＰＣＲがある場合（ＹＥＳの場合）には、ＰＣＲの位置を検出し、ＰＣＲデータをデータ保持回路４７に保持させる（ステップＮ５）。

【０１１１】そして、位置検出回路４６は、ペイロードフラグからペイロードがあるか否かを判断し（ステップＮ６）、ペイロードがある場合（ＹＥＳの場合）には、ペイロード部の開始位置を検出するまで待ち（ステップＮ７）、ペイロードがない場合（ＮＯの場合）には、動作はステップＮ１に戻る。

【０１１２】ここに、ステップＮ３において、アダプテーション・フィールドがないと判断した場合（ＮＯの場合）や、ステップＮ４において、ＰＣＲがないと判断した場合（ＮＯの場合）、動作はステップＮ６に移行する。

【０１１３】そして、ステップＮ７の後、位置検出回路４６は、ペイロード部の開始位置を検出すると、データ保持回路４７が保持するＰＣＲデータ、即ち、スクランブルしようとするペイロード部と同一のパケットのパケット・ヘッダ部のＰＣＲのデータ、あるいは、スクランブルしようとするペイロード部と同一のパケットのパケット・ヘッダ部にＰＣＲが存在しない場合には、ＰＣＲが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のＰＣＲデータを初期値として乱数発生器４５に供給するように選択回路４８を制御する（ステップＮ８）。

20

【０１１４】ここに、ＥＯＲ回路４９においては、ＭＰＥＧエンコーダ４３から入力されるストリームのうち、スクランブルの対象とされているペイロード部のストリームと、乱数発生器４５から出力される乱数とをＥＯＲ処理し、スクランブルの対象とされているペイロード部のスクランブルが行われる。

【０１１５】そして、位置検出回路４６は、選択回路５０を制御して、ＥＯＲ回路４９から出力されるスクランブルされたストリームを出力し続けさせ（ステップＮ９）、ペイロード部のストリームが終了するまで待ち（ステップＮ１０）、ステップＮ１に戻る。

【０１１６】このようにして、ＭＰＥＧエンコーダ４３から出力されるストリームは、スクランブルの対象とされているペイロード部のストリームがスクランブルされてなるストリームに変換され、ディジタル変調器５１、アップコンバータ５２、アンテナ５３、５４、チューナ５５及びディジタル復調器５６を介してデスクランブル回路５７に伝達される。

【０１１７】図８はデスクランブル回路５７の動作（本発明のデスクランブル方法の実施の第２の形態）を説明するためのフローチャートであり、デスクランブル回路５７においては、同一動作が繰り返して行われるので、選択回路６３からデスクランブルの対象とされているペイロード部、即ち、スクランブルされているペイロード部のストリームの出力を終了した時から動作を説明すると、位置検出回路５９は、ディジタル復調器５６から入力されるストリームをそのまま出力し続けるように選択回路６３を制御し、同期バイトを検出するための状態となる（ステップＱ１）。

【０１１８】そして、位置検出回路５９は、同期バイトを検出した場合、パケット・ヘッダ部のスクランブル制御の内容からペイロード部のストリームがデスクランブルの対象、即ち、スクランブルされているか否かを判断し（ステップＱ２）、スクランブルされていない場合（ＮＯの場合）には、動作はステップＱ１に戻り、位置検出回路４６は、同期バイトを検出するための状態となる。

【０１１９】これに対して、ペイロード部のストリームがスクランブルの対象とされている場合（ステップＱ２において、ＹＥＳの場合）には、位置検出回路５９は、アダプテーション・フラグからアダプテーション・フィールドがあるか否かを判断する（ステップＱ３）。

【０１２０】判断の結果、アダプテーション・フィールドがある場合（ＹＥＳの場合）には、位置検出回路５９は、ＰＣＲフラグからＰＣＲがあるか否かを判断し（ステップＱ４）、ＰＣＲがある場合（ＹＥＳの場合）には、ＰＣＲの位置を検出し、ＰＣＲデータをデータ保持回路６０に保持させる（ステップＱ５）。

【０１２１】そして、位置検出回路５９は、ペイロードフラグからペイロードがあるか否かを判断し（ステップ

21

Ｑ６）、ペイロードがある場合（ＹＥＳの場合）には、ペイロード部の開始位置を検出するまで待ち（ステップＱ７）、ペイロードがない場合（ＮＯの場合）には、動作はステップＱ１に戻る。

【０１２２】ここに、ステップＱ３において、アダプテーション・フィールドがないと判断した場合（ＮＯの場合）や、ステップＱ４において、ＰＣＲがないと判断した場合（ＮＯの場合）、動作はステップＱ６に移行する。

【０１２３】そして、ステップＱ７の後、位置検出回路５９は、ペイロード部の開始位置を検出すると、データ保持回路６０が保持するＰＣＲデータ、即ち、デスクランブルしようとするペイロード部と同一のパケットのパケット・ヘッダ部のＰＣＲのデータ、あるいは、デスクランブルしようとするペイロード部と同一のパケットのパケット・ヘッダ部にＰＣＲが存在しない場合には、ＰＣＲが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のＰＣＲデータを初期値として乱数発生器５８に供給するように選択回路６１を制御する（ステップＱ８）。

【０１２４】ここに、ＥＯＲ回路６２においては、ディジタル復調器５６から入力されるストリームのうち、スクランブルされているペイロード部のストリームと、乱数発生器５８から出力される乱数とをＥＯＲ処理し、スクランブルされているペイロード部のデスクランブルが行われる。

【０１２５】そして、位置検出回路５９は、選択回路６３を制御して、ＥＯＲ回路６２から出力されるデスクランブルされたストリームを出力し続けさせ（ステップＱ９）、ペイロード部のストリームが終了するまで待ち（ステップＱ１０）、ステップＱ１に戻る。

【０１２６】このようにして、ディジタル復調器５６から出力されるストリームは、デスクランブル回路５７において、スクランブルされているペイロード部のストリームがデスクランブルされてなるストリームに変換され、ＭＰＥＧデコーダ６４に伝達される。

【０１２７】ＭＰＥＧデコーダ６４においては、デスクランブル回路５７から伝達されるストリームから映像データのストリームと音声データのストリームとが分離されて復号化され、これら復号化された映像データ及び音声データは、テレビジョン受像機６５に伝達される。

【０１２８】このように、本発明のデータ伝達方法及びシステムの実施の第２の形態においては、ＭＰＥＧエンコーダ４３から出力されるＭＰＥＧ２－ＴＳ標準のストリームは、スクランブル回路４４において、スクランブルの対象とされているペイロード部のストリームをスクランブルしてなるストリームに変換され、デスクランブル回路５７に供給され、デスクランブルが行われて、ＭＰＥＧデコーダ６４に伝達される。

【０１２９】ここに、スクランブル回路４４においては、スクランブルの対象とされているペイロード部のストリームごとに、スクランブルしようとするペイロード部と同一のパケットのパケット・ヘッダ部のＰＣＲのデータ、あるいは、スクランブルしようとするペイロード部と同一のパケットのパケット・ヘッダ部にＰＣＲが存在しない場合には、ＰＣＲが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のＰＣＲのデータ値を初期値として乱数発生器４５に供給することにより、スクランブルの対象とされているペイロード部のストリームのスクランブルが行われる。

【０１３０】この結果、デスクランブル回路５７においては、スクランブルされているペイロード部のストリームごとに、デスクランブルしようとするペイロード部と同一のパケットのパケット・ヘッダ部のＰＣＲのデータ、あるいは、デスクランブルしようとするペイロード部と同一のパケットのパケット・ヘッダ部にＰＣＲが存在しない場合には、ＰＣＲが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のＰＣＲのデータ値を初期値として乱数発生器５８に供給することにより、スクランブルされているペイロード部のストリームのデスクランブルが行われることになる。

【０１３１】このように、本発明のデータ伝達方法及びシステムの実施の第２の形態によれば、デスクランブル回路５７の乱数発生器５８には、スクランブルされているペイロード部のストリームごとに、データ値を一定としないＰＣＲのデータ値が初期値として供給されることになるので、乱数発生器５８から発生される乱数パターンを解析することが困難となり、機密性の高いデータ伝達を実現することができる。

【０１３２】なお、この例では、ＰＣＲのデータ値を初期値として乱数発生器４５、５８に給するようにした場合について説明したが、この代わりに、たとえば、巡回カウンタのデータ値又はＰＣＲと巡回カウンタとを組み合わせ又は演算したデータのデータ値を乱数発生器４５、５８に供給するようにしても良い。

【０１３３】第３の形態・・図９

図９は本発明のデータ伝達方法の実施の第３の形態の実施に使用するデータ伝達システム（本発明のデータ伝達システムの実施の第３の形態）の要部を示すブロック図である。

【０１３４】図９中、６７は映像データを得るためのカメラ、６８は音声データを得るためのマイク、６９はカメラ６７により得られる映像データとマイク６８により得られる音声データとを符号化して時分割多重し、ＭＰＥＧ２－ＰＳ標準に基づくストリームにエンコードするＭＰＥＧエンコーダである。

【０１３５】また、７０はＭＰＥＧエンコーダ６９から出力されるストリームをスクランブルの対象とされているパケット・データ部のストリームがスクランブルされてなるストリームに変換するスクランブル回路である。

【０１３６】このスクランブル回路７０は、本発明のスクランブル方法の実施の第３の形態の実施に使用するスクランブル装置であり、本発明のスクランブル装置の実施の第３の形態をなすものである。

【０１３７】スクランブル回路７０において、７１は鍵信号により指定される系列の乱数を発生するＤＥＳ規格の乱数発生器、７２はＭＰＥＧエンコーダ６９から入力されるストリームを入力し、パケット開始コードの検出、ＰＥＳスクランブル制御の内容の確認、ＰＴＳ＆ＤＴＳフラグの内容の確認、ＰＴＳの位置検出及びパケット・データ部の開始位置検出などを行う位置検出回路である。

【０１３８】また、７３はＭＰＥＧエンコーダ６９から入力されるストリームを６４ビットの並列ストリームにパラレル変換するシリアル／パラレル変換回路（Ｓ／Ｐ）、７４はＰＴＳデータを保持する４０ビット構成のレジスタ（ＲＳ）であり、このレジスタ７４は、位置検出回路７２がＰＴＳの位置を検出すると、シリアル／パラレル変換回路７３から出力されるＰＴＳデータを保持するように位置検出回路７２により制御される。

【０１３９】また、７５は位置検出回路７２に制御され、シリアル／パラレル変換回路７３から出力されるストリームのうち、スクランブルの対象とされているパケット・データ部のストリームを保持する６４ビット構成のレジスタである。

【０１４０】また、７６はレジスタ７４が保持するＰＴＳデータ又は乱数発生器７１から出力される乱数自身を乱数発生器７１に供給する選択回路であり、この選択回路７６は、位置検出回路７２がスクランブルの対象とされているパケット・データ部の開始位置を検出すると、レジスタ７４が保持するＰＴＳデータを初期値として乱数発生器７１に供給し、その後、パケット・データ部のストリームが終了するまで、乱数発生器７１から出力される乱数をフィードバックするように位置検出回路７２により制御される。

【０１４１】なお、位置検出回路７２と、レジスタ７４と、選択回路７６とでスクランブル回路７０における初期値供給回路が構成されている。

【０１４２】また、７７はレジスタ７５から出力される並列ストリームのストリームと乱数発生器７１から出力される乱数とをＥＯＲ処理し、スクランブルの対象とされているパケット・データ部のストリームをスクランブルするＥＯＲ回路である。

【０１４３】また、７８は位置検出回路７２に制御され、ＥＯＲ回路７７から出力される並列ストリームを保持する６４ビット構成のレジスタ、７９はレジスタ７８から出力される並列ストリームをシリアル変換するパラレル／シリアル変換回路（Ｐ／Ｓ）である。

【０１４４】また、８０はＭＰＥＧエンコーダ６９から入力されるストリームとパラレル／シシアル変換回路７９から出力されるストリームとを選択して出力する選択回路であり、この選択回路８０は、ＭＰＥＧエンコーダ６９から入力されるストリームをスクランブルの対象とされているパケット・データ部のストリームがスクランブルされてなるストリームに変換したストリームを出力するように位置検出回路７２により制御される。

【０１４５】また、８１は選択回路８０から出力されるストリーム、即ち、スクランブル回路７０から出力されるストリームを蓄積するディスク等の蓄積メディア、８２は蓄積メディア８１から供給されるストリームをスクランブルされているパケット・データ部のストリームをデスクランブルしたストリームに変換するデスクランブル回路である。

【０１４６】このデスクランブル回路８２は、本発明のデスクランブル方法の実施の第３の形態の実施に使用するデスクランブル装置であり、本発明のデスクランブル装置の実施の第３の形態をなすものである。

【０１４７】デスクランブル回路８２において、８３は乱数発生器７１と同一の回路構成の乱数発生器であり、この乱数発生器８３には乱数発生器７１に使用された鍵信号と同一内容の鍵信号が供給される。

【０１４８】また、８４は蓄積メディア８１から供給されるストリームを入力し、パケット開始コードの検出、ＰＥＳスクランブル制御の内容の確認、ＰＴＳ＆ＤＴＳフラグの内容の確認、ＰＴＳの位置検出及びパケット・データ部の開始位置検出などを行う位置検出回路である。

【０１４９】また、８５は蓄積メディア８１から供給されるストリームを６４ビットの並列ストリームにパラレル変換するシリアル／パラレル変換回路、８６はＰＴＳデータを保持する４０ビット構成のレジスタであり、このレジスタ８６は、位置検出回路８４がＰＴＳの位置を検出すると、シリアル／パラレル変換回路８５から出力されるＰＴＳデータを保持するように位置検出回路８４により制御される。

【０１５０】また、８７は位置検出回路８４に制御され、シリアル／パラレル変換回路８５から出力されるスクランブルされているパケット・データ部のストリームを保持する６４ビット構成のレジスタである。

【０１５１】また、８８はレジスタ８６が保持するＰＴＳデータ又は乱数発生器８３から出力される乱数自身を乱数発生器８３に供給する選択回路であり、この選択回路８８は、位置検出回路８４がデスクランブルの対象、即ち、スクランブルされているパケット・データ部の開始位置を検出すると、レジスタ８６が保持するＰＴＳデータを初期値として乱数発生器８３に供給し、その後、パケット・データ部のストリームが終了するまで、乱数発生器８３から出力される乱数をフィードバックするように位置検出回路８４により制御される。

【０１５２】なお、位置検出回路８４と、レジスタ８６

と、選択回路８８とでデスクランブル回路８２における初期値供給回路が構成されている。

【０１５３】また、８９はレジスタ８７から出力される並列ストリームと乱数発生器８３から出力される乱数とをＥＯＲ処理し、スクランブルされているパケット・データ部のストリームをデスクランブルするＥＯＲ回路である。

【０１５４】また、９０は位置検出回路８４に制御されて、ＥＯＲ回路８９から出力される並列ストリームを保持する６４ビット構成のレジスタ、９１はレジスタ９０から出力される並列ストリームをシリアル変換するパラレル／シリアル変換回路である。

【０１５５】また、９２は蓄積メディア８１から供給されるストリームとパラレル／シリアル変換回路９１から出力されるストリームとを選択して出力する選択回路であり、この選択回路９２は、蓄積メディア８１から供給されるストリームをスクランブルされているパケット・データ部のストリームがデスクランブルされてなるストリームに変換したストリームを出力するように位置検出回路８４により制御される。

【０１５６】また、９３はデスクランブル回路８２から出力されるストリームから映像データのストリームと音声データのストリームとを分離して復号化するＭＰＥＧデコーダ、９４はＭＰＥＧデコーダ９３から出力される映像データ及び音声データが供給されるテレビジョン受像機である。

【０１５７】このデータ伝達システムにおいては、カメラ６７により得られる映像データとマイク６８により得られる音声データとは、ＭＰＥＧエンコーダ６９によって、ＭＰＥＧ２－ＰＳ標準に基づくストリームにエンコードされ、スクランブル回路７０に入力され、位置検出回路７２、シリアル／パラレル変換回路７３及び選択回路８０に供給される。

【０１５８】ここに、位置検出回路７２は、パケット開始コードを検出した場合、パケット・ヘッダ部のスクランブル制御の内容からパケット・データ部のストリームがスクランブルの対象であるか否かを判断し、スクランブルの対象とされていない場合には、パケット開始コードを検出するための状態に戻る。

【０１５９】これに対して、パケット・データ部のストリームがスクランブルの対象とされている場合には、位置検出回路７２は、パケット・ヘッダ部のＰＴＳ＆ＤＴＳフラグが“１０”又は“１１”であるか否か、即ち、ＰＴＳの有無を判断する。

【０１６０】判断の結果、ＰＴＳ＆ＤＴＳフラグが“１０”又は“１１”の場合、即ち、ＰＴＳが存在する場合には、位置検出回路７２は、ＰＴＳの位置を検出して、ＰＴＳデータをレジスタ７４に保持させ、パケット・データ部の開始位置を検出するための状態となる。

【０１６１】これに対して、ＰＴＳ＆ＤＴＳフラグが

“１０”又は“１１”以外の場合、即ち、ＰＴＳが存在しない場合には、位置検出回路７２は、そのまま、パケット・データ部の開始位置を検出するための状態となる。

【０１６２】そして、位置検出回路７２は、パケット・データ部の開始位置を検出すると、レジスタ７４が保持するＰＴＳデータ、即ち、スクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部のＰＴＳのデータ、あるいは、スクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部にＰＴＳが存在しない場合には、ＰＴＳが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のＰＴＳデータを初期値として乱数発生器７１に供給するように選択回路７６を制御すると共に、シリアル／パラレル変換回路７３から出力されるストリームをレジスタ７５に保持させる。

【０１６３】ここに、ＥＯＲ回路７７においては、レジスタ７５から出力されるストリームと乱数発生器７１から出力される乱数とをＥＯＲ処理し、スクランブルの対象とされているパケット・データ部のストリームのスクランブルが行われ、その結果がレジスタ７８に保持され、更に、レジスタ７８から出力される並列ストリームがパラレル／シリアル変換回路７９によりシリアル変換される。

【０１６４】また、位置検出回路７２は、選択回路８０を制御し、パラレル／シリアル変換回路７９から出力されるストリームを出力し続けさせ、パケット・データ部のストリームが終了するまで待ち、ＭＰＥＧエンコーダ６９から入力されるストリームをそのまま出力するように選択回路８０を制御する。

【０１６５】このようにして、ＭＰＥＧエンコーダ６９から出力されるストリームは、スクランブルの対象とされているパケット・データ部のストリームがスクランブルされてなるストリームに変換されて蓄積メディア８１に蓄積される。

【０１６６】そして、蓄積メディア８１に蓄積されたストリームは、適宜、デスクランブル回路８２に供給され、位置検出回路８４、シリアル／パラレル変換回路８５及び選択回路９２に供給される。

【０１６７】ここに、位置検出回路８４は、パケット開始コードを検出した場合、パケット・ヘッダ部のスクランブル制御の内容からパケット・データ部のストリームがデスクランブルの対象、即ち、スクランブルされているか否かを判断し、スクランブルされていない場合には、パケット開始コードを検出するための状態に戻る。

【０１６８】これに対して、パケット・データ部のストリームがスクランブルされている場合には、位置検出回路８４は、パケット・ヘッダ部のＰＴＳ＆ＤＴＳフラグが“１０”又は“１１”であるか否か、即ち、ＰＴＳの有無を判断する。

27

【０１６９】判断の結果、ＰＴＳ＆ＤＴＳフラグが“１０”又は“１１”の場合、即ち、ＰＴＳが存在する場合には、位置検出回路８４は、ＰＴＳの位置を検出して、ＰＴＳデータをレジスタ８６に保持させ、パケット・データ部の開始位置を検出するための状態となる。

【０１７０】これに対して、ＰＴＳ＆ＤＴＳフラグが“１０”又は“１１”以外の場合、即ち、ＰＴＳが存在しない場合には、位置検出回路８４は、そのまま、パケット・データ部の開始位置を検出するための状態となる。

【０１７１】そして、位置検出回路８４は、パケット・データ部の開始位置を検出すると、レジスタ８６が保持するＰＴＳデータ、即ち、デスクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部のＰＴＳのデータ、あるいは、デスクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部にＰＴＳが存在しない場合には、ＰＴＳが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のＰＴＳデータを初期値として乱数発生器８３に供給するように選択回路８８を制御すると共に、シリアル／パラレル変換回路８５から出力されるストリームをレジスタ８７に保持させる。

【０１７２】ここに、ＥＯＲ回路８９においては、レジスタ８７から出力されるストリームと乱数発生器８３から出力される乱数とをＥＯＲ処理し、スクランブルされているパケット・データ部のストリームのスクランブルが行われ、その結果がレジスタ９０に保持され、更に、レジスタ９０から出力される並列ストリームがパラレル／シリアル変換回路９１によりシリアル変換される。

【０１７３】また、位置検出回路８４は、選択回路９２を制御し、パラレル／シリアル変換回路９１から出力されるストリームを出力し続けさせ、パケット・データ部のストリームが終了するまで待ち、その後、蓄積メディア８１から供給されるストリームをそのまま出力するように選択回路９２を制御する。

【０１７４】このようにして、蓄積メディア８１から供給されるストリームは、スクランブルされているパケット・データ部のストリームがデスクランブルされてなるストリームに変換され、ＭＰＥＧデコーダ９３に伝達される。

【０１７５】ＭＰＥＧデコーダ９３においては、デスクランブル回路８２から出力されるストリームから映像データのストリームと音声データのストリームとが分離されて復号化され、テレビジョン受像機９４に伝達される。

【０１７６】このように、本発明のデータ伝達方法及びシステムの実施の第３の形態においては、ＭＰＥＧエンコーダ６９から出力されるＭＰＥＧ２－ＰＳ標準のストリームは、スクランブル回路７０において、スクランブルの対象とされているパケット・データ部のストリームをスクランブルしてなるストリームに変換され、蓄積メディア８１を介して、デスクランブル回路８２に供給され、デスクランブルが行われて、ＭＰＥＧデコーダ９３に伝達される。

28

【０１７７】ここに、スクランブル回路７０においては、ストリームを６４ビットの並列ストリームに変換し、スクランブルの対象とされているパケット・データ部のストリームごとに、スクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部のＰＴＳのデータ、あるいは、スクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部にＰＴＳが存在しない場合には、ＰＴＳが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のＰＴＳのデータ値を初期値として乱数発生器７１に供給することにより、スクランブルの対象とされているパケット・データ部のストリームのスクランブルが行われる。

【０１７８】この結果、デスクランブル回路８２においては、ストリームを６４ビットの並列ストリームに変換し、スクランブルされているパケット・データ部のストリームごとに、デスクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部のＰＴＳのデータ、あるいは、デスクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部にＰＴＳが存在しない場合には、ＰＴＳが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のＰＴＳのデータ値を初期値として乱数発生器８３に供給することにより、スクランブルされているパケット・データ部のストリームのデスクランブルが行われることになる。

【０１７９】このように、本発明のデータ伝達方法及びシステムの実施の第３の形態によれば、デスクランブル回路８２の乱数発生器８３には、スクランブルされているパケット・データ部のストリームごとに、データ値を一定としないＰＴＳのデータ値が初期値として供給されると共に、乱数発生の回数を１／６４にすることができるので、乱数発生器８３から発生される乱数パターンを解析することが困難となり、機密性の高いデータ伝達を実現することができる。

【０１８０】第４の形態・・図１０

図１０は本発明のデータ伝達方法の実施の第４の形態の実施に使用するデータ伝達システム（本発明のデータ伝達システムの実施の第４の形態）の要部を示すブロック図である。

【０１８１】図１０中、９７はパーソナル・コンピュータ、９８はデスクランブル回路の一部を構成するＰＣカード標準リリース２．０に準拠するＰＣＭＣＩＡ（Personal Computer Memory Card International Association）カードである。

【０１８２】ここに、パーソナル・コンピュータ９７に

おいて、９９はＣＰＵ（Central Processing unit）、１００は記憶回路、１０１はバス、１０２はＰＣＭＣＩＡインタフェースである。

【０１８３】また、１０３はディスク装置であり、１０４は図１に示すスクランブル回路２３から出力されるストリーム、即ち、ＭＰＥＧ２－ＰＳ標準のストリームをスクランブルの対象とされているパケット・データ部のストリームをスクランブルしてなるストリームが格納されたディスク、１０５はディスク１０４からストリームを読み取るためのディスク読取り機構である。

【０１８４】また、１０６はディスク読み取り機構１０５から読み出されたストリームを入力し、パケット開始コードの検出、ＰＥＳスクランブル制御の内容の確認、ＰＴＳ＆ＤＴＳフラグの内容の確認、ＰＴＳの位置検出及びパケット・データ部の開始位置検出などを行う位置検出回路である。

【０１８５】また、ＰＣＭＣＩＡカード９８において、１０７は鍵信号が指定する系列の乱数を発生する乱数発生器、１０８はＰＴＳデータを保持するデータ保持回路であり、このデータ保持回路１０８は、位置検出回路１０６がＰＴＳの位置を検出すると、この位置検出したＰＴＳのデータを保持するように位置検出回路１０６により制御される。

【０１８６】また、１０９はデータ保持回路１０８が保持するＰＴＳデータ又は乱数発生器１０７から出力される乱数自身を乱数発生器１０７に供給する選択回路であり、この選択回路１０９は、位置検出回路１０６がデスクランブルの対象、即ち、スクランブルされているパケット・データ部の開始位置を検出すると、データ保持回路１０８が保持するＰＴＳデータを初期値として乱数発生器１０７に供給し、その後、パケット・データ部のストリームが終了するまで、乱数発生器１０７から出力される乱数をフィードバックするように位置検出回路１０６により制御される。

【０１８７】また、１１０はディスク読み取り機構１０５から供給されるストリームのうち、スクランブルされているパケット・データ部のストリームと乱数発生器１０７から出力される乱数とをＥＯＲ処理し、スクランブルされているパケット・データ部のストリームをデスクランブルするＥＯＲ回路である。

【０１８８】また、１１１はディスク読み取り機構１０５から供給されるストリームとＥＯＲ回路１１０から出力されるストリームとを選択して出力する選択回路であり、この選択回路１１１は、ディスク読み取り機構１０５から供給されるストリームをスクランブルされているパケット・データ部のストリームがデスクランブルされてなるストリームに変換したストリームを出力するように位置検出回路１０６により制御される。

【０１８９】また、１１２はＩＤデータ（身分証明データ）等を記憶する記憶回路、１１３は記憶回路１１２からＩＤデータを出力する等の処理を行うための処理回路である。

【０１９０】ここに、位置検出回路１０６とＰＣＭＣＩＡカード９８とでデスクランブル回路が構成されているが、このデスクランブル回路は、本発明のデスクランブル装置の実施の第４の形態をなすものである。

【０１９１】また、位置検出回路１０６と、データ保持回路１０８と、選択回路１０９とで、デスクランブル回路における初期値供給回路が構成されている。なお、位置検出回路１０６は、ＰＣＭＣＩＡカード９８内に設けるようにしても良いが、この例のように、パーソナル・コンピュータ９７側に設ける場合には、ＰＣＭＣＩＡカード９８の入出力端子を減らすことができる。

【０１９２】また、パーソナル・コンピュータ９７において、１１４は選択回路１１１から出力されるストリーム、即ち、ＰＣＭＣＩＡカード９８から出力されるストリームから映像データのストリームと音声データのストリームとを分離して復号化するＭＰＥＧデコーダである。

【０１９３】また、１１５はＭＰＥＧデコーダ１１４から出力される映像データが供給されるディスプレイ、１１６はＭＰＥＧデコーダ１１４から出力される音声データが供給されるスピーカである。

【０１９４】このデータ伝達システムにおいては、パーソナル・コンピュータ９７にＰＣＭＣＩＡカード９８が入力されると、ＣＰＵ９９は、ＰＣＭＣＩＡカード９８からＩＤデータを出力させて、ＩＤデータを認証することができるか否かを判断し、認証することができる場合には、処理回路１１３に対してスクランブル回路において使用した鍵信号と同一内容の鍵信号を生成させ、乱数発生器１０７がスクランブル回路における乱数発生器と同一の系列の乱数を発生させることができるようにする。

【０１９５】そして、ディスク装置１０３が起動されると、ディスク１０４に記憶されているストリームがディスク読み出し機構１０５から出力され、位置検出回路１０６、ＰＣＭＣＩＡカード９８のデータ保持回路１０８、ＥＯＲ回路１１０及び選択回路１１１に供給される。

【０１９６】ここに、位置検出回路１０６は、パケット開始コードを検出した場合、パケット・ヘッダ部のスクランブル制御の内容からパケット・データ部のストリームがスクランブルされているか否かを判断し、スクランブルされていない場合には、パケット開始コードを検出するための状態に戻る。

【０１９７】これに対して、パケット・データ部のストリームがスクランブルされている場合には、位置検出回路１０６は、パケット・ヘッダ部のＰＴＳ＆ＤＴＳフラグが“１０”又は“１１”であるか否か、即ち、ＰＴＳの有無を判断する。

31

【０１９８】判断の結果、ＰＴＳ＆ＤＴＳフラグが“１０”又は“１１”の場合、即ち、ＰＴＳが存在する場合には、位置検出回路１０６は、ＰＴＳの位置を検出して、ＰＴＳデータをデータ保持回路１０８に保持させ、パケット・データ部の開始位置を検出するための状態となる。

【０１９９】これに対して、ＰＴＳ＆ＤＴＳフラグが“１０”又は“１１”以外の場合、即ち、ＰＴＳが存在しない場合には、位置検出回路１０６は、そのまま、パケット・データ部の開始位置を検出するための状態となる。

【０２００】そして、位置検出回路１０６は、パケット・データ部の開始位置を検出すると、データ保持回路１０８が保持しているＰＴＳデータ、即ち、デスクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部のＰＴＳのデータ、あるいは、デスクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部にＰＴＳが存在しない場合には、ＰＴＳが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のＰＴＳデータを初期値として乱数発生器１０７に供給するように選択回路１０９を制御する。

【０２０１】ここに、ＥＯＲ回路１１０においては、ディスク読み取り機構１０５から供給されるストリームのうち、デスクランブルの対象、即ち、スクランブルされているパケット・データ部のストリームと、乱数発生器１０７から出力される乱数とをＥＯＲ処理し、スクランブルされているパケット・データ部のストリームのデスクランブルが行われる。

【０２０２】また、位置検出回路１０６は、選択回路１１１を制御し、ＥＯＲ回路１１０から出力されるデスクランブルされたストリームを出力し続けさせ、パケット・データ部のストリームが終了するまで待ち、その後、ディスク読み取り機構１０５から供給されるストリームをそのまま出力するようにさせる。

【０２０３】このようにして、ディスク読み取り機構１０５から供給されるストリームは、スクランブルされているパケット・データ部のストリームがデスクランブルされてなるストリームに変換され、ＭＰＥＧデコーダ１１４に伝達される。

【０２０４】ＭＰＥＧデコーダ１１４においては、ＰＣＭＣＩＡカード９８から供給されるストリームから映像データのストリームと音声データのストリームとが分離されて復号化され、映像データは、ディスプレイ１１５に伝達され、音声データは、スピーカ１１６に伝達される。

【０２０５】このように、本発明のデータ伝達方法及びシステムの実施の第４の形態においては、ＭＰＥＧ２－ＰＳ標準のストリームをスクランブルの対象とされているパケット・データ部のストリームをスクランブルしてなるストリームが格納されたディスク１０４から読み出されたストリームは、位置検出回路１０６及びＰＣＭＣＩＡカード９８からなるデスクランブル回路によりデスクランブルされる。

32

【０２０６】ここに、位置検出回路１０６及びＰＣＭＣＩＡカード９８からなるデスクランブル回路においては、スクランブルされているパケット・データ部のストリームごとに、デスクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部のＰＴＳのデータ、あるいは、デスクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部にＰＴＳが存在しない場合には、ＰＴＳが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のＰＴＳのデータ値を初期値として乱数発生器１０７に供給することにより、スクランブルされているパケット・データ部のストリームのデスクランブルが行われる。

【０２０７】このように、本発明のデータ伝達方法及びシステムの実施の第４の形態によれば、ＰＣＭＣＩＡカード９８の乱数発生器１０７には、スクランブルされているパケット・データ部のストリームごとに、データ値を一定としないＰＴＳのデータ値が初期値として供給されると共に、ＣＰＵ９９から乱数発生器１０７に直接アクセスできないようにされているので、乱数発生器１０７から発生される乱数パターンを解析することが困難となり、機密性の高いデータ伝達を実現することができる。

【０２０８】なお、ＰＣＭＣＩＡカード９８に課金情報を持たせるようにすることができ、このようにする場合には、ディスク１０４から読み出される情報との課金が可能となる。

【０２０９】第５の形態・・図１１

図１１は本発明のデータ伝達方法の実施の第５の形態の実施に使用するデータ伝達システム（本発明のデータ伝達システムの実施の第５の形態）の要部を示すブロック図である。

【０２１０】図１１中、１１７はカメラにより得られる映像データと、マイクにより得られる音声データとを符号化して時分割多重し、ＭＰＥＧ２－ＰＳ標準又はＭＰＥＧ２－ＴＳ標準に基づくストリームにエンコードするＭＰＥＧエンコーダである。

【０２１１】また、１１８はＭＰＥＧエンコーダ１１７から出力されるストリームをスクランブルの対象とされているパケット・データ部のストリームがスクランブルされたストリームに変換するスクランブル回路である。

【０２１２】このスクランブル回路１１８は、本発明のスクランブル方法の実施の第４の形態の実施に使用するスクランブル装置であり、本発明のスクランブル装置の実施の第４の形態をなすものである。

【０２１３】スクランブル回路１１８において、１１９はＭＰＥＧエンコーダ１１７から出力されるストリーム

を格納するバッファメモリ、１２０はバッファメモリ１１９を制御するメモリコントローラ、１２１はバスである。

【０２１４】また、１２２は鍵信号により指定される系列の乱数を発生するＤＥＳ規格の乱数発生器、１２３はＭＰＥＧ２－ＰＳ標準のストリームについてのパケット開始コードの検出、ＰＥＳスクランブル制御の内容の確認、ＰＴＳ＆ＤＴＳフラグの内容の確認、ＰＴＳの位置検出、パケット・データ部の開始位置検出及びＭＰＥＧ２－ＴＳのストリームについての同期バイトの検出、アダプテーションフラグの内容の確認、ペイロードフラグの内容の確認、ＰＣＲフラグの内容の確認、ＰＣＲの位置検出、ペイロード部の開始位置検出などを行う位置検出回路などとして機能するＣＰＵである。

【０２１５】また、１２４はＭＰＥＧエンコーダ１１７から出力されるストリームがＭＰＥＧ２－ＰＳ標準の場合とＭＰＥＧ２－ＴＳ標準の場合とでＣＰＵ１２３の動作内容を変えるためのプログラムを格納するプログラムメモリである。

【０２１６】また、１２５は乱数発生器１２２に供給すべき初期値を格納する初期値レジスタであり、ＭＰＥＧエンコーダ１１７から入力されるストリームがＭＰＥＧ２－ＰＳ標準のストリームの場合にはＰＴＳデータを格納し、ＭＰＥＧ２－ＴＳ標準のストリームの場合にはＰＣＲデータを格納する。

【０２１７】また、１２６は初期値レジスタ１２５が保持するデータ値又は乱数発生器１２２から出力される乱数自身を乱数発生器１２２に供給する選択回路、１２７は選択回路１２６の選択動作を制御する選択制御レジスタである。

【０２１８】ここに、選択回路１２６は、ＣＰＵ１２３がスクランブルの対象とされているパケット・データ部又はペイロード部の開始位置を検出すると、初期値レジスタが保持する初期値を乱数発生器１２２に供給し、その後、パケット・データ部又はペイロード部のストリームが終了するまで、乱数発生器１２２から出力される乱数をフィードバックするように選択制御レジスタ１２７の出力値により制御される。

【０２１９】また、１２８はバッファメモリ１１９から読み出されるストリームを格納するデータ・レジスタ、１２９はデータ・レジスタ１２８から出力されるパケット・データ部又はペイロード部のストリームと乱数発生器１２２から出力される乱数とをＥＯＲ処理し、スクランブルの対象とされているパケット・データ部又はペイロード部のストリームをスクランブルするＥＯＲ回路である。

【０２２０】また、１３０はデータ・レジスタ１２８から出力されるストリームと、ＥＯＲ回路１２９から出力されるストリームとを選択して出力する選択回路であり、この選択回路１３０は、データ・レジスタ１２８から出力されるストリームをスクランブルの対象とされているパケット・データ部又はペイロード部のストリームがスクランブルされてなるストリームに変換したストリームを出力するように制御される。

【０２２１】また、１３１は選択回路１３０から出力されるストリーム、即ち、スクランブル回路１１８から出力されるストリームを蓄積するディスク等の蓄積メディアである。

【０２２２】また、１３２は蓄積メディア１３１から供給されるストリームを、スクランブルされているパケット・データ部又はペイロード部のストリームがデスクランブルされてなるストリームに変換するデスクランブル回路である。

【０２２３】このデスクランブル回路１３２は、本発明のデスクランブル方法の実施の第５の形態の実施に使用するデスクランブル装置であり、本発明のデスクランブル装置の実施の第５の形態をなすものである。

【０２２４】このデスクランブル回路１３２において、１３３は蓄積メディア１３１から出力されるストリームを格納するバッファメモリ、１３４はバッファメモリ１３３を制御するメモリコントローラ、１３５はバスである。

【０２２５】また、１３６は乱数発生器１２２と同一の回路構成の乱数発生器であり、この乱数発生器１３６には乱数発生器１２２に使用された鍵信号と同一内容の鍵信号が供給される。

【０２２６】また、１３７はＭＰＥＧ２－ＰＳ標準のストリームについてのパケット開始コードの検出、ＰＥＳスクランブル制御の内容の確認、ＰＴＳ＆ＤＴＳフラグの内容の確認、ＰＴＳの位置検出、パケット・データ部の開始位置検出及びＭＰＥＧ２－ＴＳ標準のストリームについての同期バイトの検出、アダプテーションフラグの内容の確認、ペイロードフラグの内容の確認、ＰＣＲフラグの内容の確認、ＰＣＲの位置検出、ペイロード部の開始位置検出などを行う位置検出回路などとして機能するＣＰＵである。

【０２２７】また、１３８は蓄積メディア１３１から供給されるストリームがＭＰＥＧ２－ＰＳ標準の場合とＭＰＥＧ２－ＴＳ標準の場合とでＣＰＵ１３７の動作内容を変えるためのプログラムを格納するプログラムメモリである。

【０２２８】また、１３９は乱数発生器１３６に供給すべき初期値を格納する初期値レジスタであり、蓄積メディア１３１から供給されるストリームがＭＰＥＧ２－ＰＳ標準のストリームの場合にはＰＴＳデータを格納し、ＭＰＥＧ２－ＴＳ標準のストリームの場合にはＰＣＲデータを格納する。

【０２２９】また、１４０は初期値レジスタ１３９が保持するデータ値又は乱数発生器１３６から出力される乱数自身を乱数発生器１３６に供給する選択回路、１４１

は選択回路１４０の選択動作を制御する選択制御レジスタである。

【０２３０】ここに、選択回路１４０は、ＣＰＵ１３７がスクランブルされているパケット・データ部又はペイロード部の開始位置を検出すると、初期値レジスタ１３９が保持する初期値を乱数発生器１３６に供給し、その後、パケット・データ部又はペイロード部のストリームが終了するまで、乱数発生器１３６から出力される乱数をフィードバックするように選択制御レジスタ１４１の出力値により制御される。

【０２３１】また、１４２はバッファメモリ１３３から読み出されるストリームを格納するデータ・レジスタ、１４３はデータ・レジスタ１４２から出力されるパケット・データ部又はペイロード部のストリームと乱数発生器１３６から出力される乱数とをＥＯＲ処理し、スクランブルされているパケット・データ部又はペイロード部のストリームをデスクランブルするＥＯＲ回路である。

【０２３２】また、１４４はデータ・レジスタ１４２から出力されるストリームと、ＥＯＲ回路１４３から出力されるストリームとを選択して出力する選択回路であり、この選択回路１４４は、データ・レジスタ１４２から出力されるストリームをスクランブルされているパケット・データ部又はペイロード部のストリームがデスクランブルされてなるストリームに変換したストリームを出力するように制御される。

【０２３３】また、１４５はデスクランブル回路１３２から出力されるストリームから映像データのストリームと音声データのストリームとを分離して復号化するＭＰＥＧデコーダである。

【０２３４】このデータ伝達システムにおいては、カメラにより得られる映像データとマイクにより得られる音声データとは、ＭＰＥＧエンコーダ１１７によって、ＭＰＥＧ２－ＰＳ標準又はＭＰＥＧ２－ＴＳ標準に基づくストリームにエンコードされ、スクランブル回路１１８に伝達される。

【０２３５】そして、スクランブル回路１１８に供給されるストリームは、バッファメモリ１１９に格納され、バッファメモリ１１９に格納されたストリームは、ＣＰＵ１２３により読み出される。

【０２３６】ここに、ＭＰＥＧエンコーダ１１７から出力されるストリームがＭＰＥＧ２－ＰＳ標準のストリームである場合には、ＣＰＵ１２３は、パケット開始コードの検出、ＰＥＳスクランブル制御の内容の確認、ＰＴＳ＆ＤＴＳの内容の確認、ＰＴＳの位置検出及びパケット・データ部の開始位置検出などを行う。

【０２３７】そして、ＣＰＵ１２３は、パケット開始コードを検出した場合、パケット・ヘッダ部のスクランブル制御の内容からパケット・データ部のストリームがスクランブルの対象とされているか否かを判断し、スクランブルの対象とされていない場合には、パケット開始コードを検出するための状態に戻る。

【０２３８】これに対して、パケット・データ部のストリームがスクランブルの対象とされている場合には、ＣＰＵ１２３は、パケット・ヘッダ部のＰＴＳ＆ＤＴＳフラグが“１０”又は“１１”であるか否か、即ち、ＰＴＳの有無を判断する。

【０２３９】判断の結果、ＰＴＳ＆ＤＴＳフラグが“１０”又は“１１”の場合、即ち、ＰＴＳが存在する場合には、ＣＰＵ１２３は、ＰＴＳの位置を検出して、ＰＴＳデータを初期値レジスタ１２５に保持させ、パケット・データ部の開始位置を検出するための状態となる。

【０２４０】これに対して、ＰＴＳ＆ＤＴＳフラグが“１０”又は“１１”以外の場合、即ち、ＰＴＳが存在しない場合には、ＣＰＵ１２３は、そのまま、パケット・データ部の開始位置を検出するための状態となる。

【０２４１】そして、ＣＰＵ１２３は、パケット・データ部の開始位置を検出すると、初期値レジスタ１２５が保持するＰＴＳデータ、即ち、スクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部のＰＴＳのデータ、あるいは、スクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部にＰＴＳが存在しない場合には、ＰＴＳが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のＰＴＳデータを初期値として乱数発生器１２２に供給するように選択制御レジスタ１２７の書換えを行う。

【０２４２】ここに、ＥＯＲ回路１２９においては、データ・レジスタ１２８から出力されるストリームのうち、スクランブルの対象とされているパケット・データ部のストリームと、乱数発生器１２２から出力される乱数とがＥＯＲ処理され、スクランブルの対象とされているパケット・データ部のストリームのスクランブルが行われる。

【０２４３】この場合、ＣＰＵ１２３は、選択回路１３０を制御し、ＥＯＲ回路１２９から出力されるスクランブルされたストリームを出力し続けさせ、パケット・データ部のストリームが終了するまで待ち、パケット開始コードを検出するための状態に戻る。

【０２４４】このようにして、ＭＰＥＧエンコーダ１１７から出力されるストリームは、スクランブルの対象とされているパケット・データ部のストリームがスクランブルされてなるストリームに変換されて蓄積メディア１３１に蓄積され、この蓄積メディア１３１に蓄積されたストリームは、適宜、デスクランブル回路１３２に供給されることになる。

【０２４５】ここに、デスクランブル回路１３２に供給されるストリームは、バッファメモリ１３３に格納され、バッファメモリ１３３に格納されたストリームは、ＣＰＵ１３７により読み出される。

【０２４６】そして、ＣＰＵ１３７は、パケット開始コ

ードを検出した場合、パケット・ヘッダ部のスクランブル制御の内容からパケット・データ部のストリームがスクランブルされているか否かを判断し、スクランブルされていない場合には、パケット開始コードを検出するための状態に戻る。

【０２４７】これに対して、パケット・データ部のストリームがスクランブルされている場合には、ＣＰＵ１３７はパケット・ヘッダ部のＰＴＳ＆ＤＴＳフラグが“１０”又は“１１”であるか否か、即ち、ＰＴＳの有無を判断する。

【０２４８】判断の結果、ＰＴＳ＆ＤＴＳフラグが“１０”又は“１１”の場合、即ち、ＰＴＳが存在する場合には、ＣＰＵ１３７は、ＰＴＳの位置を検出して、ＰＴＳデータを初期値レジスタ１３９に保持させ、パケット・データ部の開始位置を検出するための状態となる。

【０２４９】これに対して、ＰＴＳ＆ＤＴＳフラグが“１０”又は“１１”以外の場合、即ち、ＰＴＳが存在しない場合には、ＣＰＵ１３７は、そのまま、パケット・データ部の開始位置を検出するための状態となる。

【０２５０】そして、ＣＰＵ１３７は、パケット・データ部の開始位置を検出すると、初期値レジスタ１３９が保持するＰＴＳデータ、即ち、デスクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部のＰＴＳのデータ、あるいは、デスクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部にＰＴＳが存在しない場合には、ＰＴＳが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のＰＴＳデータを初期値として乱数発生器１３６に供給するように選択制御レジスタ１４１の書換えを行う。

【０２５１】ここに、ＥＯＲ回路１４３においては、データ・レジスタ１４２から出力されるストリームのうち、スクランブルされているパケット・データ部のストリームと、乱数発生器１３６から出力される乱数とがＥＯＲ処理され、スクランブルされているパケット・データ部のストリームのデスクランブルが行われる。

【０２５２】この場合、ＣＰＵ１３７は、選択回路１４４を制御し、ＥＯＲ回路１４３から出力されるデスクランブルされたストリームを出力し続けさせ、パケット・データ部のストリームが終了するまで待ち、パケット開始コードを検出するための状態に戻る。

【０２５３】このようにして、蓄積メディア１３１から出力されるストリームは、スクランブルの対象とされているパケット・データ部のストリームがスクランブルされてなるストリームに変換され、ＭＰＥＧデコーダ１４５に伝達される。

【０２５４】他方、ＭＰＥＧエンコーダ１１７からＭＰＥＧ２－ＴＳ標準のストリームが出力される場合には、ＣＰＵ１２３は同期バイトの検出を行い、パケット・ヘッダ部のスクランブル制御の内容からペイロード部のストリームがスクランブルの対象とされているか否かを判断し、スクランブルの対象とされていない場合には、同期バイトを検出するための状態に戻る。

【０２５５】これに対して、ペイロード部のストリームがスクランブルの対象とされている場合には、ＣＰＵ１２３は、アダプテーションフラグからアダプテーション・フィールドがあるか否かを判断し、アダプテーション・フィールドがない場合には、ＣＰＵ１２３は、ペイロードフラグからペイロードがあるか否かを判断する。

【０２５６】これに対して、アダプテーション・フィールドがある場合には、ＣＰＵ１２３は、ＰＣＲフラグからＰＣＲがあるか否かを判断し、ＰＣＲがない場合には、ペイロードフラグからペイロードがあるか否かを判断する。

【０２５７】これに対して、ＰＣＲがある場合には、ＣＰＵ１２３は、ＰＣＲの位置を検出し、ＰＣＲデータを初期値レジスタ１２５に保持させ、ペイロードフラグからペイロードがあるか否かを判断する。

【０２５８】ここに、ＣＰＵ１２３は、ペイロードがない場合には、同期バイトを検出するための状態となり、ペイロードがある場合には、ペイロード部の開始位置を検出するための状態となる。

【０２５９】そして、ＣＰＵ１２３は、ペイロード部の開始位置を検出すると、初期値レジスタ１２５が保持するＰＣＲデータ、即ち、スクランブルしようとするペイロード部と同一のパケットのパケット・ヘッダ部のＰＣＲのデータ、あるいは、スクランブルしようとするペイロード部と同一のパケットのパケット・ヘッダ部にＰＣＲが存在しない場合には、ＰＣＲが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のＰＣＲデータを初期値として乱数発生器１２２に供給するように選択制御レジスタ１２７の書換えを行う。

【０２６０】ここに、ＥＯＲ回路１２９においては、データ・レジスタ１２８から出力されるストリームのうち、スクランブルの対象とされているペイロード部のストリームと、乱数発生器１２２から出力される乱数とをＥＯＲ処理し、スクランブルの対象とされているペイロード部のストリームのスクランブルが行われる。

【０２６１】この場合、ＣＰＵ１２３は、選択回路１３０を制御して、ＥＯＲ回路１２９から出力されるスクランブルされたストリームを出力し続けさせ、ペイロード部のストリームが終了するまで待ち、同期バイトを検出するための状態に戻る。

【０２６２】このようにして、ＭＰＥＧエンコーダ１１７から出力されるストリームは、スクランブルの対象とされているパケット・データ部のストリームがスクランブルされてなるストリームに変換されて蓄積メディア１３１に蓄積され、この蓄積メディア１３１に蓄積されたストリームは、適宜、デスクランブル回路１３２に供給されることになる。

【０２６３】ここに、デスクランブル回路１３２に供給されるストリームは、バッファメモリ１３３に格納され、バッファメモリ１３３に格納されたストリームは、ＣＰＵ１３７により読み出される。

【０２６４】ここに、ＣＰＵ１３７は、同期バイトの検出を行い、パケット・ヘッダ部のスクランブル制御の内容からペイロード部のストリームがスクランブルされているか否かを判断し、スクランブルされていない場合には、同期バイトを検出するための状態に戻る。

【０２６５】これに対して、ペイロード部のストリームがスクランブルされている場合には、ＣＰＵ１３７は、アダプテーションフラグからアダプテーション・フィールドがあるか否かを判断し、アダプテーション・フィールドがない場合には、ペイロードフラグからペイロードがあるか否かを判断する。

【０２６６】これに対して、アダプテーション・フィールドがある場合には、ＣＰＵ１３７は、ＰＣＲフラグからＰＣＲがあるか否かを判断し、ＰＣＲがない場合には、ペイロードフラグからペイロードがあるか否かを判断する。

【０２６７】これに対して、ＰＣＲがある場合には、ＣＰＵ１３７は、ＰＣＲの位置を検出し、ＰＣＲデータを初期値レジスタ１３９に保持させ、ペイロードフラグからペイロードがあるか否かを判断する。

【０２６８】ここに、ＣＰＵ１３７は、ペイロードがない場合には、同期バイトを検出するための状態となり、ペイロードがある場合には、ペイロード部の開始位置を検出するための状態となる。

【０２６９】そして、ＣＰＵ１３７は、ペイロード部の開始位置を検出すると、初期値レジスタ１３９が保持するＰＣＲデータ、即ち、デスクランブルしようとするペイロード部と同一のパケットのパケット・ヘッダ部のＰＣＲのデータ、あるいは、デスクランブルしようとするペイロード部と同一のパケットのパケット・ヘッダ部にＰＣＲが存在しない場合には、ＰＣＲが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のＰＣＲデータを初期値として乱数発生器１３６に供給するように選択制御レジスタ１４１の書換えを行う。

【０２７０】ここに、ＥＯＲ回路１４３においては、データ・レジスタ１４２から出力されるストリームのうち、スクランブルされているペイロード部のストリームと、乱数発生器１３６から出力される乱数とをＥＯＲ処理し、スクランブルされているペイロード部のストリームのデスクランブルが行われる。

【０２７１】この場合、ＣＰＵ１３７は、選択回路１４４を制御して、ＥＯＲ回路１４３から出力されるデスクランブルされたストリームを出力し続けさせ、ペイロード部のストリームが終了するまで待ち、同期バイトを検出するための状態に戻る。

【０２７２】このようにして、蓄積メディア１３１から

出力されるストリームは、デスクランブル回路１３２において、スクランブルされているペイロード部のストリームがデスクランブルされてなるストリームに変換され、ＭＰＥＧデコーダ１４５に伝達される。

【０２７３】このように、本発明のデータ伝達方法及びシステムの実施の第５の形態においては、ＭＰＥＧエンコーダ１１７から出力されるＭＰＥＧ２－ＰＳ標準又はＭＰＥＧ２－ＴＳ標準のストリームは、スクランブル回路１１８において、パケット・データ部又はペイロード部のストリームをスクランブルしてなるストリームに変換され、蓄積メディア１３１を介して、デスクランブル回路１３２に供給され、デスクランブルが行われて、ＭＰＥＧデコーダ１４５に伝達される。

【０２７４】ここに、スクランブル回路１１８においては、スクランブルの対象とされているパケット・データ部又はペイロード部のストリームごとに、スクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部のＰＴＳのデータ、あるいは、スクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部にＰＴＳが存在しない場合には、ＰＴＳが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のＰＴＳデータ、又は、スクランブルしようとするペイロード部と同一のパケットのパケット・ヘッダ部のＰＣＲのデータ、あるいは、スクランブルしようとするペイロード部と同一のパケットのパケット・ヘッダ部にＰＣＲが存在しない場合には、ＰＣＲが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のＰＣＲデータを初期値として乱数発生器１２２に供給することによって、スクランブルの対象とされているパケット・データ部又はペイロード部のストリームのスクランブルが行われる。

【０２７５】この結果、デスクランブル回路１３２においては、スクランブルされているパケット・データ部又はペイロード部のストリームごとに、デスクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部のＰＴＳのデータ、あるいは、デスクランブルしようとするパケット・データ部と同一のパケットのパケット・ヘッダ部にＰＴＳが存在しない場合には、ＰＴＳが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のＰＴＳデータ、又は、デスクランブルしようとするペイロード部と同一のパケットのパケット・ヘッダ部のＰＣＲのデータ、あるいは、デスクランブルしようとするペイロード部と同一のパケットのパケット・ヘッダ部にＰＣＲが存在しない場合には、ＰＣＲが存在するパケット・ヘッダ部のうち、直前のパケット・ヘッダ部のＰＣＲデータを初期値として乱数発生器１２２に供給することによって、デスクランブルの対象とされているパケット・データ部又はペイロード部のストリームのデスクランブルが行われる。

【０２７６】このように、本発明のデータ伝達方法及び

システムの実施の第５の形態によれば、デスクランブル回路１３２の乱数発生器１３６には、スクランブルされているパケット・データ部又はペイロード部のストリームごとに、データ値を一定としないＰＴＳ又はＰＣＲのデータ値が初期値として供給されることになるので、乱数発生器１３６から発生される乱数パターンを解析することが困難となり、機密性の高いデータ伝達を実現することができると共に、ＭＰＥＧ２－ＰＳシステム及びＭＰＥＧ２－ＴＳシステムの２系列の伝送系に適用することができるので、利便性を高めることができる。

【０２７７】

【発明の効果】以上のように、本発明のスクランブル方法を使用する場合には、デスクランブルは、スクランブルされている第２のストリーム部ごとに、第１のストリーム部内のデータ値が一定でない所定のデータを初期値として乱数発生器に供給することにより行われることになり、デスクランブル側の乱数発生器には、スクランブルされている第２のストリーム部ごとに、値を一定としない初期値が供給されることになるので、乱数発生器から発生される乱数パターンを解析することが困難となり、機密性の高いデータ伝達を実現することができる。

【０２７８】また、本発明のスクランブル装置を使用する場合には、デスクランブル装置は、乱数を発生する乱数発生器と、スクランブルされている第２のストリーム部ごとに、第１のストリーム部内のデータ値が一定でない所定のデータを初期値として乱数発生器に供給する初期値供給回路と、スクランブルされている第２のストリーム部と乱数発生器から出力される乱数とを論理演算してスクランブルされている第２のストリーム部をデスクランブルする論理演算回路とを備えて構成されることになり、デスクランブル装置の乱数発生器には、スクランブルされている第２のストリーム部ごとに、値を一定としない初期値が供給されることになるので、乱数発生器から発生される乱数パターンを解析することが困難となり、機密性の高いデータ伝達を実現することができる。

【０２７９】また、本発明のデスクランブル方法によれば、乱数発生器には、スクランブルされている第２のストリーム部ごとに、値を一定としない初期値が供給されることになるので、乱数発生器から発生される乱数パターンを解析することが困難となり、機密性の高いデータ伝達を実現することができる。

【０２８０】また、本発明のデスクランブル装置によれば、乱数発生器には、スクランブルされている第２のストリーム部ごとに、必ずしも値を一定としない初期値が供給されることになるので、乱数発生器から発生される乱数パターンを解析することが困難となり、機密性の高いデータ伝達を実現することができる。

【０２８１】また、本発明のデータ伝達方法によれば、本発明のスクランブル方法及び本発明のデスクランブル方法を使用しているので、機密性の高いデータ伝達を実現することができる。

【０２８２】また、本発明のデータ伝達装置によれば、本発明のスクランブル装置及び本発明のデスクランブル装置を使用しているので、機密性の高いデータ伝達を実現することができる。

【図面の簡単な説明】

【図１】本発明のデータ伝達方法の実施の第１の形態の実施に使用するデータ伝達システム（本発明のデータ伝達システムの実施の第１の形態）の要部を示すブロック図である。

【図２】ＭＰＥＧ２－ＰＳのＰＥＳパケットの構造を示す図である。

【図３】図１に示す本発明のデータ伝達システムの実施の第１の形態が備えるスクランブル回路の動作を説明するためのフローチャートである。

【図４】図１に示す本発明のデータ伝達システムの実施の第１の形態が備えるデスクランブル回路の動作を説明するためのフローチャートである。

【図５】本発明のデータ伝達方法の実施の第２の形態の実施に使用するデータ伝達システム（本発明のデータ伝達システムの実施の第２の形態）の要部を示すブロック図である。

【図６】ＭＰＥＧ２－ＴＳのトランスポート・パケットの構造を示す図である。

【図７】図５に示す本発明のデータ伝達システムの実施の第２の形態が備えるスクランブル回路の動作を説明するためのフローチャートである。

【図８】図５に示す本発明のデータ伝達システムの実施の第２の形態が備えるデスクランブル回路の動作を説明するためのフローチャートである。

【図９】本発明のデータ伝達方法の実施の第３の形態の実施に使用するデータ伝達システム（本発明のデータ伝達システムの実施の第３の形態）の要部を示すブロック図である。

【図１０】本発明のデータ伝達方法の実施の第４の形態の実施に使用するデータ伝達システム（本発明のデータ伝達システムの実施の第４の形態）の要部を示すブロック図である。

【図１１】本発明のデータ伝達方法の実施の第５の形態の実施に使用するデータ伝達システム（本発明のデータ伝達システムの実施の第５の形態）の要部を示すブロック図である。

【図１２】従来のデータ伝達システムの一例の要部を示すブロック図である。

【図１３】図１２に示すデータ伝達システムが有する問題点を説明するための図である。

【符号の説明】

２２、４３、６９、１１７　ＭＰＥＧエンコーダ

３８、６４、９３、１１４、１４５　ＭＰＥＧデコーダ

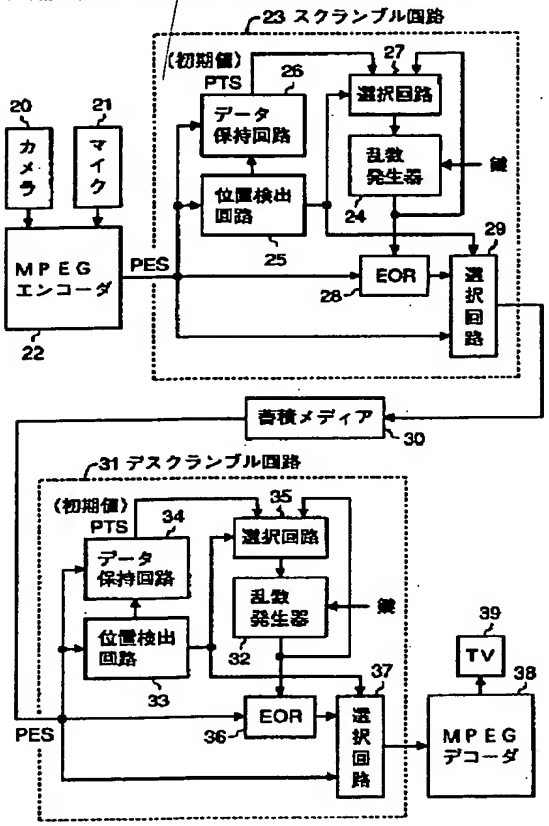
２３、４４、７０、１１８　スクランブル回路

43　　44

３１、５７、８２、１３２　デスクランブル回路

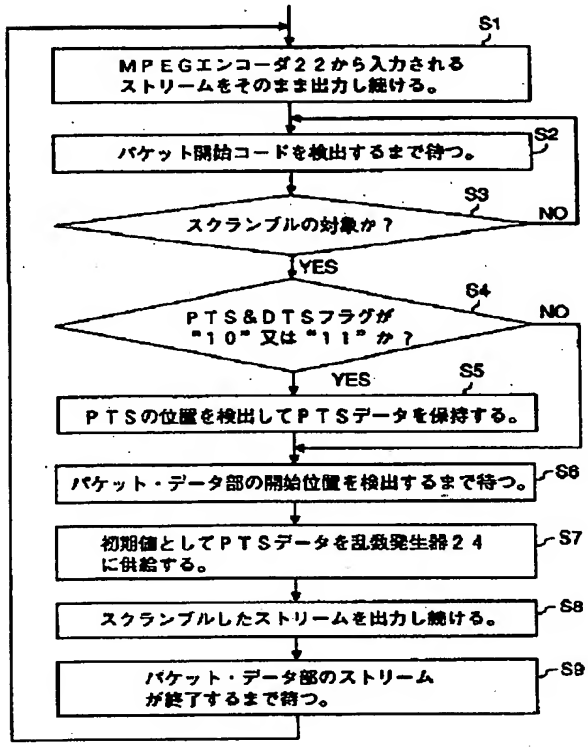
【図１】

本発明のデータ伝達方法の実施の第１の形態の実施に使用するデータ伝達システム（本発明のデータ伝達システムの実施の第１の形態）の要部を示すブロック図



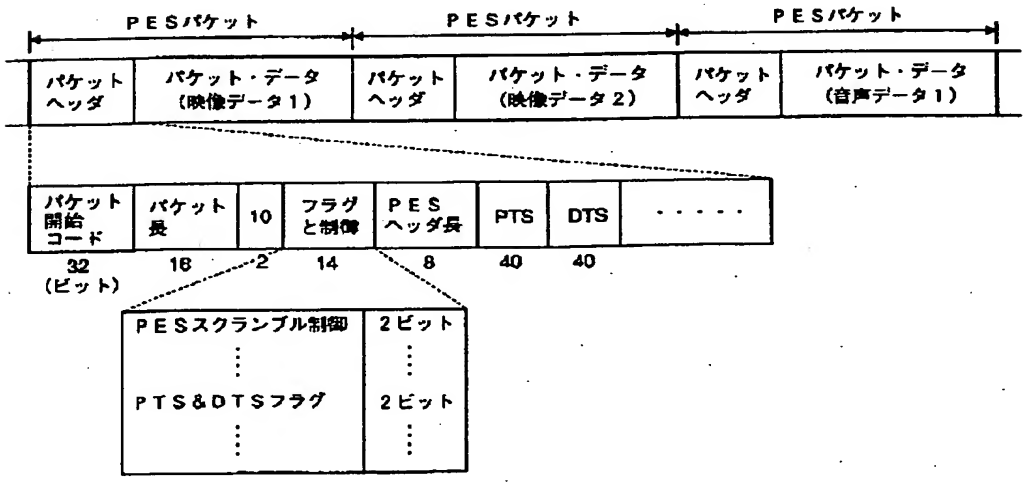
【図３】

スクランブル回路２３の動作（本発明のスクランブル方法の実施の第１の形態）を説明するためのフローチャート



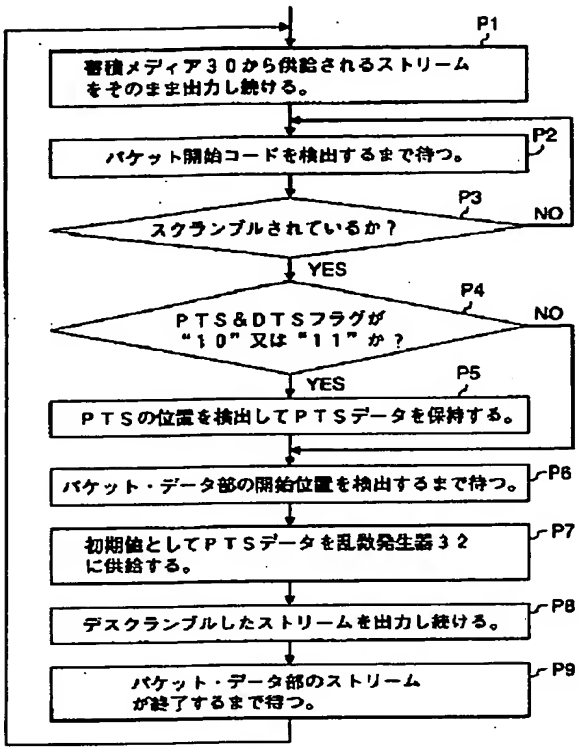
【図２】

MPEG２－PSのPESパケットの構造を示す図



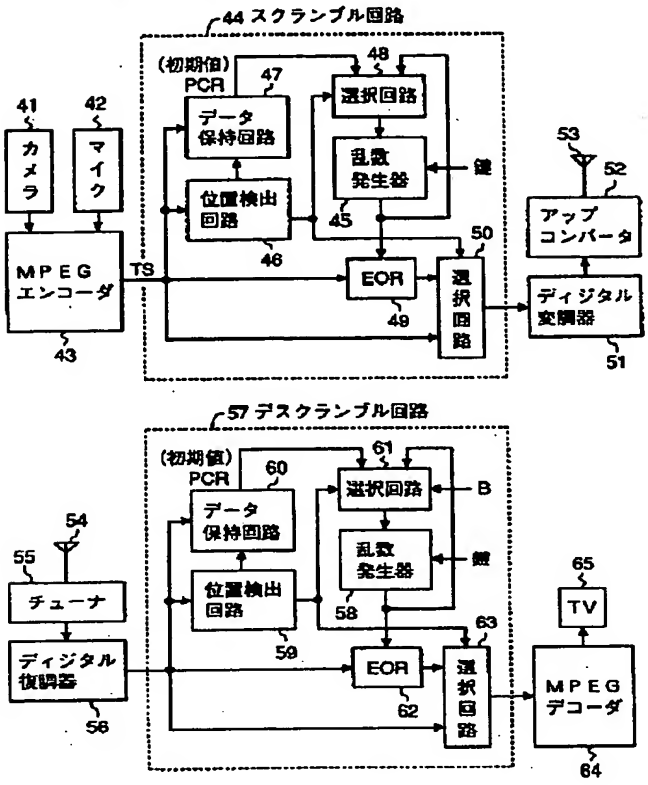
【図４】

デスクランブル回路３１の動作（本発明のデスクランブル方法の実施の第１の形態）を説明するためのフローチャート



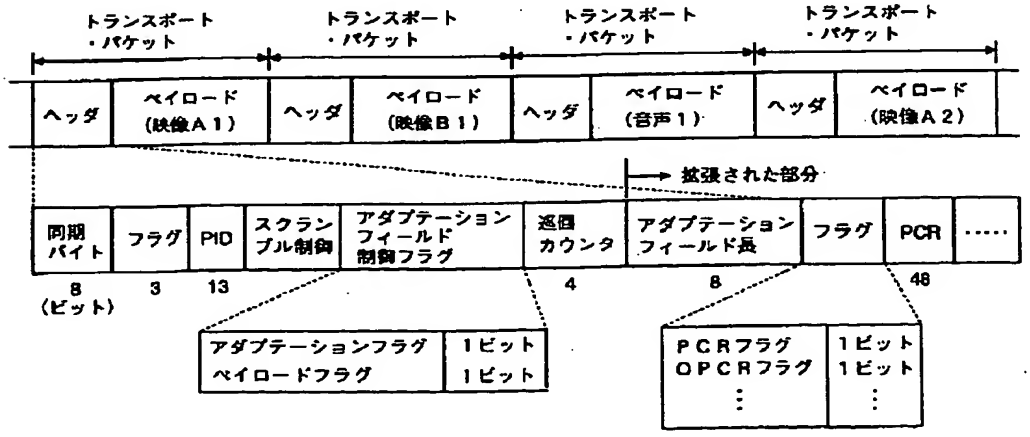
【図５】

本発明のデータ伝送方法の実施の第２の形態の実施に使用するデータ伝送システム（本発明のデータ伝送システムの実施の第２の形態）の要部を示すブロック図



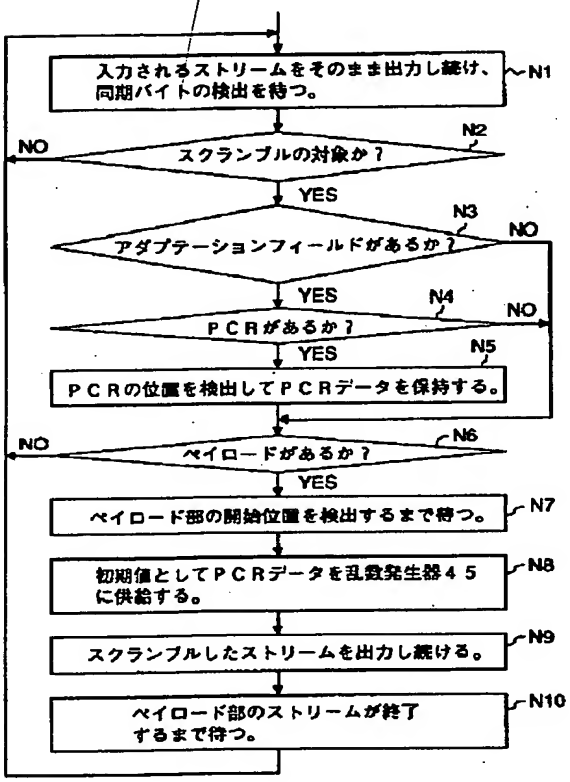
【図６】

MPEG２－TSのトランスポート・パケットの構造を示す図



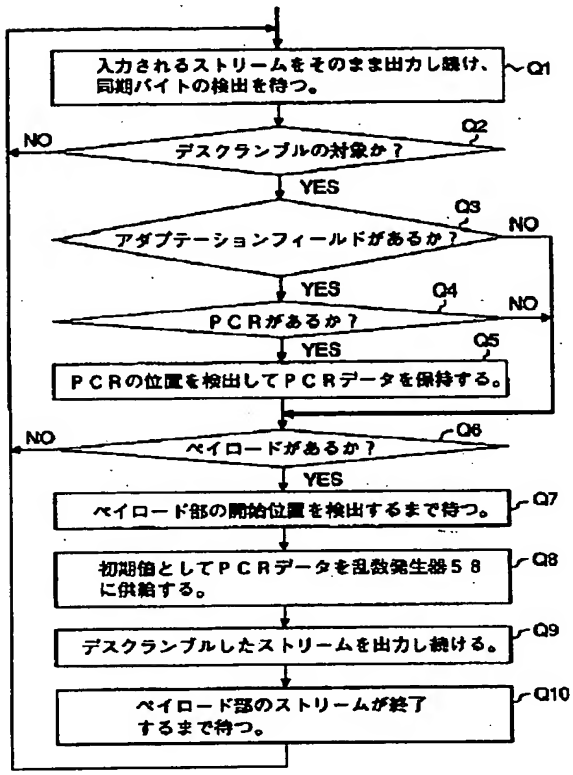
【図７】

スクランブル回路４４の動作（本発明のスクランブル方法の実施の第２の形態）を説明するためのフローチャート



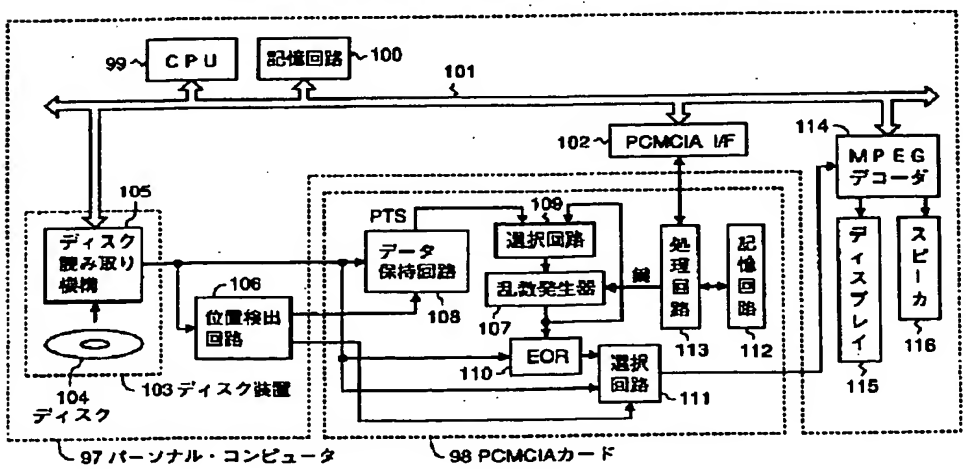
【図８】

デスクランブル回路５７の動作（本発明のデスクランブル方法の第２の形態）を説明するためのフローチャート



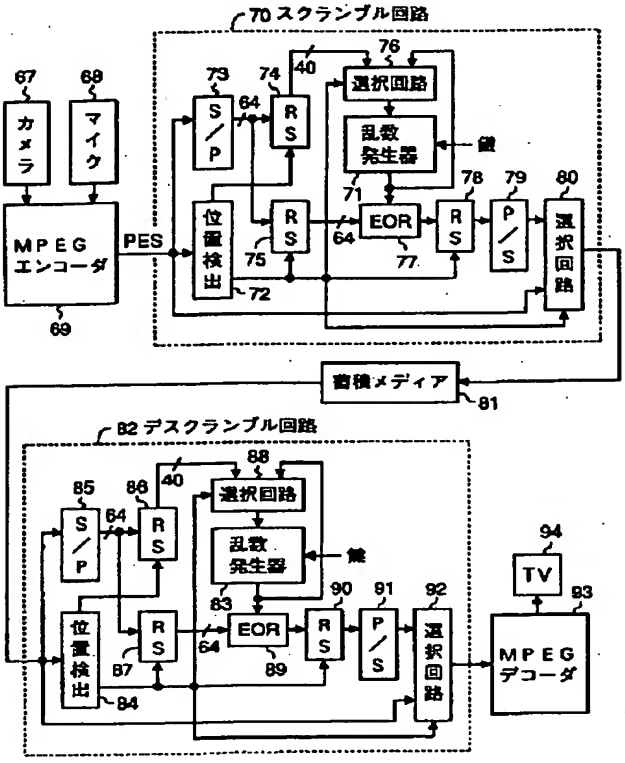
【図１０】

本発明のデータ伝達方法の実施の第４の形態の実施に使用するデータ伝達システム（本発明のデータ伝達システムの実施の第４の形態）の要部を示すブロック図



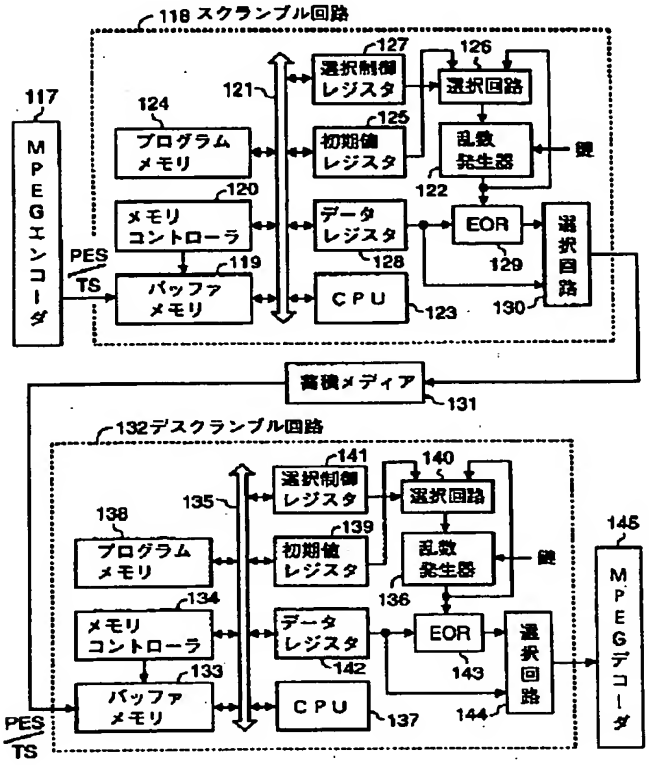
【図９】

本発明のデータ伝送方法の実施の第３の形態の実施に使用するデータ伝送システム（本発明のデータ伝送システムの実施の第３の形態）の要部を示すブロック図



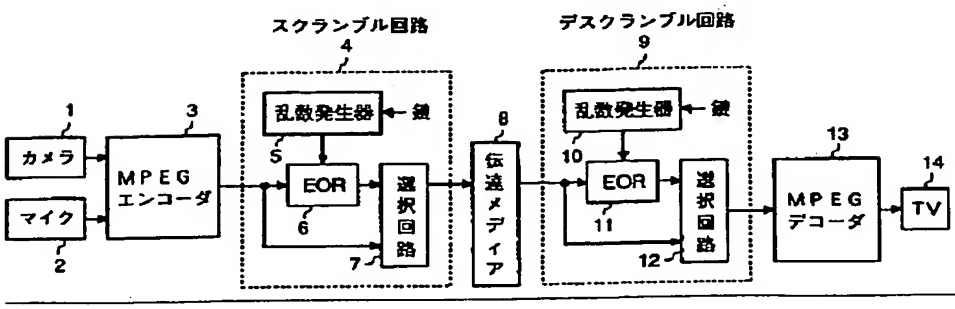
【図１１】

本発明のデータ伝送方法の実施の第５の形態の実施に使用するデータ伝送システム（本発明のデータ伝送システムの実施の第５の形態）の要部を示すブロック図



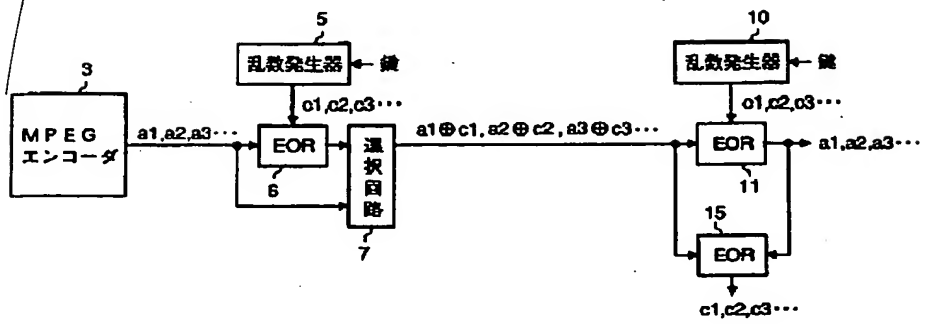
【図１２】

従来のデータ伝送システムの一例の要部を示すブロック図



【図１３】

図１２に示す従来のデータ伝送システム
が有する問題点を説明するための図



フロントページの続き

(72)発明者　秋山　良太
神奈川県川崎市中原区上小田中１０１５番
地　富士通株式会社内
(72)発明者　飯島　清克
神奈川県川崎市中原区上小田中１０１５番
地　富士通株式会社内